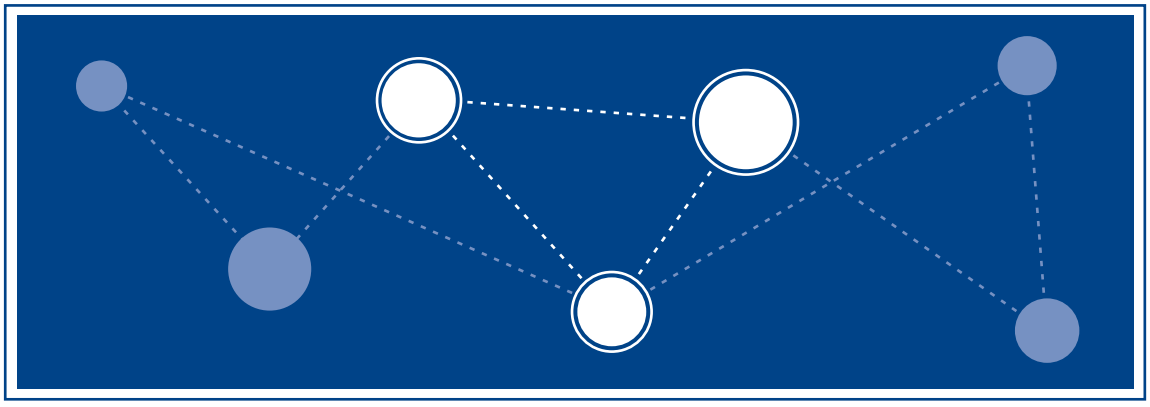


NETSCREEN
INSTANT VIRTUAL EXTRANET
PLATFORM

ADMINISTRATIONSHANDBUCH

NETSCREEN®

NetScreen Secure Access
NetScreen-SA 1000
NetScreen-SA 3000
NetScreen-SA 5000
NetScreen-SA FIPS

NetScreen Secure Meeting
NetScreen-SM 3000

NETSCREEN
INSTANT VIRTUAL EXTRANET
PLATTFORM

ADMINISTRATIONSHANDBUCH

Copyright © 2004 NetScreen Technologies, Inc. Alle Rechte vorbehalten.

NetScreen, NetScreen Technologies, GigaScreen und das NetScreen-Logo sind eingetragene Marken von NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC und NetScreen ScreenOS sind Marken von NetScreen Technologies, Inc. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Firmen. Die Angaben in diesem Dokument können ohne vorherige Ankündigung geändert werden. Ohne Vorliegen einer schriftlichen Genehmigung darf kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht. Die schriftliche Genehmigung erfolgt durch: NetScreen Technologies, Inc., Building #3, 805 11th Avenue, Sunnyvale, CA 94089, www.netscreen.com.

Warnung: Änderungen oder Modifikationen an diesem Produkt können zum Erlöschen der Garantie und der Betriebserlaubnis für das Gerät führen. Haftungsausschluss: DIE SOFTWARELIZENZ UND EINGESCHRÄNKTE GARANTIE FÜR DAS BEILIEGENDE PRODUKT SIND IM INFORMATIONSPAKET NIEDERGELEGT, DAS IM LIEFERUMFANG DES PROKUKTS ENTHALTEN IST, UND WIRD DURCH DIESEN HINWEIS BESTANDTEIL DES VERTRAGS. WENN SIE DIE SOFTWARELIZENT ODER DIE EINGESCHRÄNKTE GARANTIE NICHT FINDEN KÖNNEN, ERHALTEN SIE EINE KOPIE VON IHREM NETSCREEN-HÄNDLER.

Copyright © 2001 D. J. Bernstein. Copyright © 1985-2003 Massachusetts Institute of Technology. Alle Rechte vorbehalten. Copyright © 2000 Zero-Knowledge Systems, Inc. Copyright © 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. Alle Rechte vorbehalten. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1989, 1991, 1992 Carnegie Mellon University. Derivative Work - 1996, 1998-2000. Copyright © 1996, 1998-2000 The Regents of the University of California. Alle Rechte vorbehalten. Copyright © 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. Alle Rechte vorbehalten. Das Kopieren und Verteilen wortgetreuer Kopien dieses Dokuments ist gestattet. Copyright © 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. Alle Rechte vorbehalten. Copyright © 1986 Gary S. Brown. Copyright © 1998 CORE SDI S.A., Buenos Aires, Argentina. Copyright © 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Copyright © 1998-2002. The OpenSSL Project. Alle Rechte vorbehalten. Copyright © 1989-2001, Larry Wall. Alle Rechte vorbehalten. Copyright © 1989, 1991 Free Software Foundation, Inc. Copyright © 1996-2002 Andy Wardley. Alle Rechte vorbehalten. Copyright © 1998-2002. Canon Research Centre Europe Ltd. Copyright © 1995-1998. Jean-loup Gailly and Mark Adler.

Secure Access Product Group
NetScreen Technologies, Inc.
940 Stewart Drive
Sunnyvale, CA 94085, USA
Telefon: 408-962-8200
Fax: 408-962-8201

400A020404

Inhalt

Vorwort ix

Teil 1. IVE Series 1

Einführung in das NetScreen Instant Virtual Extranet 3

Access Series – Übersicht 7

Access Series FIPS – Übersicht 9

Secure Meeting – Übersicht 13
Konferenzplanung, -teilnahme und -durchführung 14
Zugriff auf den Konferenz-URL 17
Von Secure Meeting unterstützte Umgebungen 18
Secure Meeting – Fehlerbehebung 20

Zugriffsverwaltung – Übersicht 23
Richtlinien, Regeln und Einschränkungen sowie Bedingungen 23
Angeben von Sicherheitsanforderungen 26

Authentifizierungsbereiche – Übersicht 35
Authentifizierungsserver 35
Authentifizierungsrichtlinien 36
Verzeichnisserver 37
Rollenzuordnungsregeln 37

Ressourcenrichtlinien – Übersicht 41
Angeben von Ressourcen für eine Ressourcenrichtlinie 45
Schreiben einer detaillierten Regel 52

Benutzerrollen – Übersicht 55

Teil 2. IVE-Funktionen 61

Cachebereinigung – Übersicht 63

Central Manager – Übersicht 67

Zertifikate – Übersicht 69
Serverzertifikate 69
Clientzertifikate 70
Appletzertifikate 71

Cluster – Übersicht 75
Cluster – Übersicht 75
Bereitstellen eines Clusterpaars im Aktiv/Passiv-Modus 76
Bereitstellen eines Clusterpaars oder eines Clusters mit mehreren Einheiten im Aktiv/Aktiv-Modus 78
Statussynchronisierung 79
Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung 81

Delegierte Administration – Übersicht 83

E-Mail-Client – Übersicht 85
Auswählen eines E-Mail-Clients 86
Arbeiten mit einem standardbasierten Mailserver 86
Arbeiten mit Microsoft Exchange Server 87
Arbeiten mit Lotus Notes und Lotus Notes Mail Server 90

Hostprüfung – Übersicht 91

Protokollierung und Überwachung – Übersicht 95
Schweregrade der Protokolldatei 96
Benutzerdefinierte Filterung von Protokolldateien 97

Network Connect – Übersicht 99

Durchgangsproxy – Übersicht 103

Remote SSO – Übersicht 107

Secure Application Manager – Übersicht 109
Windows Secure Application Manager (W-SAM) – Übersicht 109
Java Secure Application Manager (J-SAM) – Übersicht 111
Erweiterte Unterstützung für MS Exchange 116
Erweiterte Unterstützung für Lotus Notes 119
Erweiterte Unterstützung für Citrix NFuse 120

Teil 3. IVE-Konfiguration 123

Konfigurieren der Seite „Status“ 125
Registerkarte „Overview“ 125
Registerkarte „Active Users“ 131
Registerkarte „Meeting Schedule“ 133

Konfigurieren der Seite „Schedule“ 136

Konfigurieren der Seite „Configuration“ 137
Registerkarte „Licensing“ 137
Registerkarte „Security > Security Options“ 140
Registerkarte „Security > Host Checker“ 143
Registerkarte „Security > Cache Cleaner“ 146
Registerkarte „Certificates > Server Certificate“ 147
Registerkarte „Certificates > CA Certificate“ 153
Registerkarte „Certificates > Applet Certificates“ 155

Konfigurieren der Seite „Network“ 157
Registerkarte „Internal Port“ 157
Registerkarte „External Port“ 161
Registerkarte „Static Routes“ 163
Registerkarte „Hosts“ 164

Konfigurieren der Seite „Clustering“ 167
Registerkarte „Create“ 168
Registerkarte „Status“ 170
Registrierkarte „Join“ 175
Verfahren über die serielle Konsole 179
Registerkarte „Properties“ 182

Konfigurieren der Seite „Log Monitoring“ 187
Registerkarten „Events“, „User Access“ und „Admin Access“ 187
Registerkarte „SNMP“ 195
Registerkarte „Statistics“ 200

Konfigurieren der Seite „Signing-in“ 203
Registerkarte „Sign-in Policies“ 203
Registerkarte „Sign-in Page“ 209
Registrierkarte „Server“ 212
Konfigurieren einer ACE/Serverinstanz 215

Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz 221
Konfigurieren einer Instanz eines anonymen Servers 223
Konfigurieren einer Zertifikatserverinstanz 225
Konfigurieren einer LDAP-Serverinstanz 229
Konfigurieren einer lokalen IVE-Server-Instanz 235
Konfigurieren einer NIS-Serverinstanz 241
Konfigurieren einer RADIUS-Serverinstanz 243
Konfigurieren einer Netegrity SiteMinder-Instanz 247
Anzeigen und Löschen von Benutzersitzungen 263

Konfigurieren der Seite „Delegation“ 265
Registerkarte „General“ 268
Registerkarte „System“ 268
Registerkarte „User Role Admin“ 271

Konfigurieren eines Authentifizierungsbereichs 273
Registerkarte „General“ 273
Registerkarte „Authentication Policy“ 275
Registerkarte „Role Mapping“ 277

Konfigurieren der Seite „Roles“ 285
Registerkarte „General > Overview“ 286
Registerkarte „General > Restrictions“ 287
Registerkarte „General > Session Options“ 289
Registerkarte „General > UI Options“ 293
Registerkarte „Web > Bookmarks“ 294
Registerkarte „Web > Options“ 296
Registerkarte „Files > Windows Bookmarks“ 299
Registerkarte „Files > UNIX Bookmarks“ 301
Registerkarte „Files > Options“ 302
Registerkarte „SAM > Applications“ 304
Registerkarte „SAM > Options“ 312
Registerkarte „Telnet/SSH > Sessions“ 315
Registerkarte „Telnet/SSH > Options“ 316
Registerkarte „Meetings“ 317
Registerkarte „Network Connect“ 322

Konfigurieren der Seite „New User“ 323

Konfigurieren der Seite „Web“ 325
Registerkarte „Access“ 330
Registerkarte „Caching > Policies“ 331
Registerkarte „Caching > Options“ 335
Registerkarte „Java > Access Control“ 336
Registerkarte „Java > Code Signing“ 337
Registerkarte „Rewriting > Selective Rewriting“ 339
Registerkarte „Rewriting > Pass-through Proxy“ 340
Registerkarte „Remote SSO > Form POST“ 342
Registerkarte „Remote SSO > Headers/Cookies“ 345
Registerkarte „Web Proxy > Policies“ 346
Registerkarte „Web Proxy > Settings“ 348

Konfigurieren der Seite „Files“ 351
Registerkarte „Windows > Access“ 352
Registerkarte „Windows > Credentials“ 355
Registerkarte „UNIX/NFS“ 358
Registerkarte „Encoding“ 360

Konfigurieren der Seite „SAM“ 361

Konfigurieren der Seite „Telnet/SSH“ 365

Konfigurieren der Seite „Network Connect“ 369
Registerkarte „Access“ 370
Registerkarte „IP Address Pools“ 373

Konfigurieren der Seite „Meetings“ 375

Konfigurieren der Seite „Email Client“ 379

Konfigurieren der Seite „System“ 383
Registerkarte „Platform“ 383
Registerkarte „Upgrade/Downgrade“ 384
Registerkarte „Options“ 386

Konfigurieren der Seite „Import/Export“ 389
Registerkarte „Configuration“ 389
Registerkarte „User Accounts“ 393
Registerkarte „Roles and Policies“ 394

Konfigurieren der Seite „Push Config“ 399

Konfigurieren der Seite „Archiving“ 403
Registerkarte „FTP Server“ 403
Registerkarte „Local Backups“ 406

Konfigurieren der Seite „Troubleshooting“ 409
Registerkarte „Policy Tracing“ 409
Registerkarte „Session Recording“ 413
Registerkarte „System Snapshot“ 414
Registerkarte „TCP Dump“ 415
Registerkarte „Commands“ 417
Registerkarte „Remote Debugging“ 418

Chapter 4. Zusatzinformationen 421

Appendix A. Authentifizierung und Autorisierung – Flussdiagramm 423

Appendix B. Konfigurieren der Zugriffsverwaltungsoptionen 427
Quell-IP-Einschränkungen 428
Browsereinschränkungen 429
Zertifikateinschränkungen 431
Kennworteinschränkung 433
Hostprüfungseinstellungen 434
Cachebereinigungseinschränkungen 435

Appendix C. Schreiben benutzerdefinierter Ausdrücke 437
Systemvariablen und Beispiele 442

Appendix D. Verwenden der seriellen Konsole des IVE 453

Index 465

Vorwort

In diesem Handbuch finden Sie die erforderlichen Informationen zum Konfigurieren und Verwalten des NetScreen Instant Virtual Extranet (IVE), unter anderem zu den folgenden Themen:

- Übersicht über die Access Series-Produkte und das zugrunde liegende Zugriffsverwaltungssystem
- Übersicht über Basis- und erweiterte Funktionen sowie über Aktualisierungsoptionen
- Anweisungen für die Konfiguration und Verwaltung der IVE-Appliance oder des IVE-Clusters

Zielgruppe

Dieses Handbuch wendet sich an Systemadministratoren, die für die Konfiguration eines Access Series-Produkts zuständig sind.

NetScreen-SA 1000
NetScreen-SA 3000
NetScreen-SA 5000
NetScreen-SA FIPS
NetScreen-SM 3000

Weiterführende Informationen

Informationen zur Installation können Sie dem Installationshandbuch entnehmen, dass dem Produkt beiliegt. Den neuesten Build des IVE-Betriebssystems mit dem zugehörigen *Administrationshandbuch* im PDF-Format und den Versionshinweisen können Sie unter http://support.netscreen.com herunterladen.

Informationen über eine Aktualisierung der Konfiguration finden Sie unter „www.netscreen.com“, oder schreiben Sie eine E-Mail an „sales@neoteris.com“.

x

Teil 1
IVE Series

In diesem Abschnitt werden die NetScreen IVE-Plattform (Instant Virtual Extranet), die Access Series-Produktlinien, die auf dieser Plattform aufbauen, und das Zugriffsverwaltungssystem beschrieben, das von den Access Series-Produkten verwendet wird.

Inhalt

Einführung in das NetScreen Instant Virtual Extranet 3
Access Series – Übersicht 7
Access Series FIPS – Übersicht 9
Secure Meeting – Übersicht 13
Zugriffsverwaltung – Übersicht 23
Authentifizierungsbereiche – Übersicht 35
Ressourcenrichtlinien – Übersicht 41
Benutzerrollen – Übersicht 55

Einführung in das NetScreen Instant Virtual Extranet

Mit dem NetScreen Instant Virtual Extranet können Sie Mitarbeitern, Partnern und Kunden über einen beliebigen Webbrowser überall sicheren und kontrollierten Zugriff auf Datei- und Webserver des Unternehmens, systemeigene Nachrichten- und E-Mail-Clients, gehostete Server und vieles mehr gewähren.

Was ist das NetScreen Instant Virtual Extranet?

Das NetScreen Instant Virtual Extranet oder IVE ist eine gehärtete Netzwerkappliance, die solide Sicherheitsfunktionen bietet. Sie fungiert als Zwischenglied für die Datenströme, die zwischen externen Benutzern und internen Ressourcen übertragen werden. Zu diesen gehören:

- MS Terminal-Server
- MS Exchange-Server
- Lotus Notes-Server
- Internet-E-Mail-Server
- Terminalbasierte Anwendungen (IBM 3270, VT100)
- Dokumente auf Dateiservern
- Webbasierte Unternehmensanwendungen
- Intranetseiten

Mit dem IVE wird es überflüssig, in einer herkömmlichen DMZ Toolkits für Extranets bereitzustellen oder den Mitarbeitern ein VPN (Virtual Private Network) für Remotezugriffe zur Verfügung zu stellen. Die Appliance vermittelt Daten zwischen externen Verbindungen, über die sie sichere Anforderungen erhält, und internen Ressourcen, an die sie Anforderungen für authentifizierte Benutzer sendet.

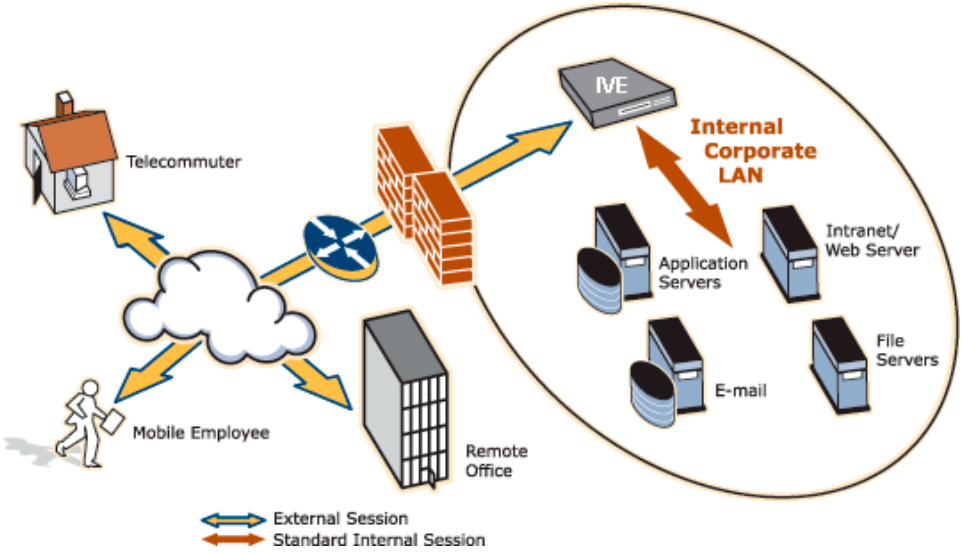


Abbildung 1:Die IVE-Appliance innerhalb eines LAN

Wie funktioniert das IVE?

Das IVE arbeitet als sicheres Gateway auf Anwendungsebene, das sämtliche Anforderungen zwischen dem öffentlichen Internet und internen Unternehmensressourcen vermittelt. Sämtliche Anforderungen, die das Instant Virtual Extranet erhält, wurden bereits durch im Browser des Endbenutzers per 128-Bit- oder 168-Bit-SSL/HTTPS verschlüsselt. Unverschlüsselte Anforderungen werden verworfen. Jede Anforderung unterliegt der vom Administrator definierten Zugriffssteuerung, bei der z.B. 2-Faktor-Authentifizierung oder clientseitige digitale Zertifikate eingesetzt werden, bevor sie an die internen Ressourcen weitergeleitet wird. Da das IVE eine stabile Sicherheitsschicht zwischen dem öffentlichen Internet und den internen Ressourcen zur Verfügung stellt, müssen Administratoren nicht fortwährend Sicherheitsrichtlinien verwalten und Sicherheitslücken für zahlreiche verschiedene Anwendungen und Webserver beheben, die in der öffentlichen DMZ bereitgestellt werden.

Das Instant Virtual Extranet vermittelt den Zugriff auf verschiedenste Arten von Anwendungen und Ressourcen mithilfe einfacher Webbrowsertechnologien. Die Benutzer erhalten über eine durch die Appliance gehostete Extranetsitzung einen authentifizierten Zugriff auf autorisierte Ressourcen. Benutzer können von jedem Webbrowser mit Internetanbindung über eine sichere Websitzung auf umfangreiche webbasierte Unternehmensanwendungen, Java-

Anwendungen, Dateifreigaben, Terminalhosts und weitere Client/Server-Anwendungen (wie z. B. Microsoft Outlook und Lotus Notes) zugreifen.

Wie wird das IVE konfiguriert?

Die Konfiguration des IVE erfolgt in fünf grundlegenden Schritten über die Webkonsole des Administrators:

1. **Definieren von Benutzer und Administratorrollen.**

   Seiten der Webkonsole:
   User > Roles und **Administrators > Delegation**

   Rollensteuerung, auf die Ressourcenbenutzer und Administratoren zugreifen können. Sie können z. B. eine Rolle erstellen, die Benutzern den Zugriff auf Netzwerkverzeichnisse erlaubt und gleichzeitig den Webzugang verweigert.

   Auf dem IVE sind bereits eine Benutzerrolle („Users") und zwei Administratorenrollen („.Administrators" und „.Read-Only Administrators") vorkonfiguriert.

2. **Definieren von Ressourcenrichtlinien.**

   Seiten der Webkonsole: **Ressourcenrichtlinien**

   Ressourcenrichtlinien dienen zur weiter gehenden Steuerung der Ressourcen, auf die Benutzer und Administratoren zugreifen können. Wenn Sie z. B. den Dateizugriff auf Rollenebene aktiviert haben, können Sie eine Ressourcenrichtlinie erstellen, die den Zugriff auf bestimmte Verzeichnisse im Firmennetzwerk verweigert. Bei der Konfiguration einer Ressourcenrichtlinie müssen Sie die Rollen angeben, für die Ressourcenrichtlinie gelten soll.

   Das IVE ist mit Ressourcenrichtlinien vorkonfiguriert, die allen Benutzern die Web- und Dateisuche erlaubt.

3. **Definieren von Authentifizierungs- und Autorisierungsservern.**

   Seiten der Webkonsole: **System > Signing In > Servers**

   Authentifizierungs- und Autorisierungsserver authentifizieren Anmeldeinformationen und ermitteln die Benutzerberechtigungen innerhalb des Systems. Sie können z. B. Benutzer anhand der clientseitigen Zertifikatsattribute über einen einen Zertifikatsserver authentifizieren und dann einen LDAP-Server erstellen, der Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind.

   Auf dem IVE sind bereits ein lokaler Server für die Benutzerauthentifizierung („System Local") und ein lokaler Server für die Administratorauthentifizierung („Administrators") vorkonfiguriert. Sie müssen also zumindest diesen Servern Benutzer hinzufügen, um den Benutzern Zugriff auf das IVE zu erlauben.

4. **Definieren des Authentifizierungsbereichs.**

   Seiten der Webkonsole:
   Users > Authentication und **Administrators > Authentication**

   Authentifizierungsbereiche enthalten Richtlinien, die die Bedingungen festlegen, die Benutzer und Administratoren für die Anmeldung am IVE erfüllen müssen. Sie können z. B. anhand einer Authentifizierungsrichtlinie angeben, dass Benutzer nur auf das IVE zugreifen können, wenn sie sich von einer bestimmten IP-Adresse aus anmelden oder einen bestimmten Browser verwenden. Beim Konfigurieren eines Authentifizierungsbereichs müssen Sie Regeln erstellen, um Benutzer zu Rollen zuzuordnen und festzulegen, welche(n) Server das IVE für die Authentifizierung und Autorisierung der Bereichsmitglieder verwenden darf.

   Auf dem IVE ist bereits ein Bereich („Users") vorkonfiguriert, der alle über den Server „System Local" authentifizierten Benutzer zur Rolle „Users" zuordnet. Außerdem ist auf dem IVE bereits ein Bereich („Admin Users") vorkonfiguriert, der alle über den Server „.Administrators" authentifizierten Benutzer zur Rolle „Administrators" zuordnet.

5. **Definieren von Anmelderichtlinien.**

   Seite der Webkonsole: **System > Signing In > Sign-In Policies**

   Anmelderichtlinien definieren die URLs, die Benutzer und Administratoren für die Anmeldung am IVE verwenden können. Sie können z. B. Anmelderichtlinien verwenden, um einen Anmelde-URL für die Abteilung „Vertrieb" und einen anderen für die Abteilung „Versand" zu erstellen. Bei der Konfiguration einer Anmelderichtlinie müssen Sie diese mindestens einem Bereich zuordnen. Es können sich dann nur Mitglieder des angegebenen Bereichs bzw. der angegebenen Bereiche anhand des URLs, der in der Richtlinie angegeben wurde, am IVE anmelden.

   Auf dem IVE ist bereits eine Anmelderichtlinie vorkonfiguriert, die den Benutzern des Bereichs „Admin Users" erlaubt, sich anhand des URL „*/admin" anzumelden, sowie eine weitere, die den Benutzern des Bereichs „Users" gestattet, sich anhand des URL „*/" anzumelden.

Access Series – Übersicht

Die NetScreen Access™ Series-Produktfamilie bietet ein hohes Maß an Skalierbarkeit für Unternehmen, hohe Verfügbarkeit sowie Sicherheitsfunktionen, um den sicheren Zugriff auf Netzwerkressourcen zu erweitern. Das Access Series Instant Virtual Extranet (IVE) kann innerhalb weniger Stunden konfiguriert werden, um Benutzern sicheren Zugriff auf die folgenden Elemente zu ermöglichen:

- Interne Unternehmenswebsites und webbasierte Anwendungen, darunter clientseitige Java-Applets, unter Verwendung von Desktopcomputern, Laptopcomputern und drahtlosen Pocket PC-Geräten (Standard)
- Interne Dateiserver (NFS und CIFS) des Unternehmens sowie Funktionen zur Dateiübertragung an und von beliebigen Verzeichnissen (Standard)
- Systemeigene Nachrichtenclients wie Microsoft Outlook und IBM/Lotus Notes von jedem PC aus (Aktualisierungsoption für Secure Email Client)
- Auf Standards basierende E-Mail-Clients wie Microsoft Outlook Express, Netscape Communicator und Eudora von Qualcomm von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Client-/Serveranwendungen wie Citrix ICA Client, pcAnywhere und MS-Terminaldienste von jedem PC aus (Aktualisierungsoption für Secure Application Manager)
- Gehostete Server über Telnet und SSH von jedem PC aus (Aktualisierungsoption für sicheren Terminalzugriff)
- Funktionen für die sichere Zusammenarbeit, einschließlich der Planung von Konferenzen, Remote-Konferenzvorführungen, Remotesteuerung des Desktops des Vorführenden sowie Textchats (Aktualisierungsoption Secure Meeting)

Ihre Mitarbeiter, Partner und Kunden benötigen lediglich einen Standardwebbrowser für den PC (Internet Explorer/Netscape/AOL/Pocket IE) und eine Internetverbindung für den Zugriff auf die intuitive Startseite des Access Series IVE. Auf dieser Seite wird das Fenster bereitgestellt, über das die Benutzer sicher Web- oder Dateiserver durchsuchen, HTML-fähige Unternehmensanwendungen verwenden, den Client-/Serveranwendungsproxy starten oder eine Terminalsitzung beginnen können[1].

Die Installation, Konfiguration und Verwaltung des IVE sind unkompliziert. Bei dem IVE handelt es sich um eine Netzwerkappliance, die innerhalb

1. Die verfügbaren Funktionen hängen von dem erworbenen Produkt der NetScreen Access Series und den erworbenen Aktualisierungsoptionen ab.

weniger Minuten im Rack montiert werden kann. Sobald eine Verbindung mit Ihrem Netzwerk besteht, müssen Sie an der seriellen Konsole nur noch einige System- und Netzwerkeinstellungen eingeben, um auf die Webkonsole zuzugreifen. Die Webkonsole ist die Webschnittstelle, über die Sie das IVE nach den Anforderungen Ihres Unternehmens konfigurieren und verwalten können. Die folgenden Features ermöglichen eine problemlose Bereitstellung und effiziente Wartung des Systems:

- Einfache Serverintegration – Das IVE lässt sich in vorhandene Authentifizierungsserver (LDAP, RADIUS, NIS, Windows NT-Domäne, Active Directory und RSA-ACE/Server) des Unternehmens integrieren. Sie müssen keine Änderungen an den internen Webservern, Dateiservern oder Netzwerken vornehmen.
- Zertifikatauthentifizierung – Schützt Anwendungen ohne Änderungen an den internen Ressourcen. Sie wählen lediglich die digitalen Zertifikate als Teil des Authentifizierungsschemas für das Access Series IVE aus.
- Hohe Verfügbarkeit und Redundanz – Keine Ausfallzeit für die Benutzer im seltenen Fall eines Systemausfalls und „Stateful Peering", durch das die Benutzereinstellungen, die Systemeinstellungen und die Sitzungsdaten der Benutzer synchronisiert werden (in einer Cluster-Umgebung).
- Einfache Firewallrichtlinien – Von außen ist nur SSL-Zugriff auf die IVE-Appliance erforderlich.
- Ressourcenzugriffskontrolle auf der Ebene der Dateien und URLs, die das IVE 4.0 Zugriffsverwaltungssystem verwenden (Authentifizierungsbereiche, Benutzerrollen und Ressourcenrichtlinien)
- Zentralisierte Protokollierung auf Anwendungsebene, durch die Administrator- und Benutzeraktionen, Verbindungs-, Datei- und Webanforderungen sowie Systemfehler verfolgt werden.
- Systemsoftwareaktualisierungen über das Internet.
- SNMP- und DMZ-Unterstützung.

Access Series FIPS – Übersicht

FIPS oder ***Federal Information Processing Standards (Bundesstandards für Informationsverarbeitung)*** sind Bestimmungen des NIST (National Institute of Standards and Technology) für die Behandlung von Schlüsseln und verschlüsselten Daten. NetScreen Access Series FIPS ist ein Standard-A5000- oder A3000-NetScreen Instant Virtual Extranet, das mit einem Kryptographiemodul mit FIPS-Zertifikat ausgerüstet ist. Das auf einem Access Series FIPS-System installierte manipulationssichere Hardwaresicherheitsmodul erfüllt die Sicherheitsanforderungen des FIPS 140-2-Zertifikats der Ebene 3. Das Modul verwaltet private Kryptographieschlüssel und führt SSL-Handshakes durch. Dabei stellt es die Kompatibilität mit FIPS sicher und delegiert rechenintensive PKI-Aufgaben (Public Key Infrastructure) von der Appliance an das dedizierte Modul.

Administratoren müssen für Access Series FIPS-Geräte im Prinzip die gleichen Konfigurationsaufgaben wie für IVEs durchführen, die nicht dem FIPS-Standard entsprechen. Nur bei der Initialisierung, Clusterbildung und Zertifikatserzeugung sind kleinere Konfigurationsänderungen erforderlich. Für die wenigen Fälle, in denen die Verwaltungsaufgaben abweichen, enthält dieses Handbuch die entsprechenden Anweisungen für Access Series- und Access Series FIPS-Administratoren. Für Endbenutzer gibt es keine Unterschiede zwischen einem Access Series FIPS-System und einem IVE-Standardsystem.

Wie funktioniert NetScreen Access Series FIPS?

Bei der Erstinstallation eines Access Series FIPS-Systems werden Sie über die serielle Konsole des IVE durch die Schritte zum Einrichten einer Security World geführt. Eine ***Security World*** ist ein von Access Series FIPS verwendetes Schlüsselmanagementsystem, das sich aus den folgenden Elementen zusammensetzt:

- **Kryptographiemodul** – Das Kryptographiemodul (auch als Hardwaresicherheitsmodul oder HSM bezeichnet) von Access Series FIPS enthält Hardware und Firmware, die direkt in der Appliance installiert wird. Eine Security World kann aus einem einzelnen Kryptographiemodul (Standardumgebung) oder verschiedenen Modulen (Clusterumgebung) bestehen. Eine einzelne Access Series FIPS-Appliance ist aber immer mit einem Kryptographiemodul ausgestattet.
- **Security World-Schlüssel** – Ein Security World-Schlüssel ist ein eindeutig verschlüsselter Triple DES-Schlüssel, der die Sicherheit aller anderen Anwendungsschlüssel in einer Security World gewährleistet. Die Federal Information Processing Standards (FIPS) schreiben vor, dass dieser Schlüssel nicht in eine Security World importiert werden kann, son-

dern direkt in einem Kryptographiemodul erzeugt werden muss. In einer Clusterumgebung verwenden alle Module in der Security World denselben Security World-Schlüssel. (Weitere Informationen finden Sie unter „Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung“ auf Seite 81.)

- **Smartcards** – Eine Smartcard ist ein transportabler Schlüssel, der wie eine Kreditkarte aussieht. Benutzer können sich mithilfe einer Smartcard authentifizieren, um auf verschiedene Daten und Prozesse, die vom Kryptographiehardwaremodul gesteuert werden, zuzugreifen. Beim Initialisierungsvorgang muss der mit dem Kryptographiemodul gelieferte Smartcardleser angeschlossen und dann eine Smartcard in den Leser eingelegt werden. Während des Initialisierungsvorgangs wird die Smartcard in eine ***Administratorkarte*** umgewandelt, die dem Karteninhaber den Zugriff auf die Security World gestattet. (Weitere Informationen finden Sie unter „Erstellen weiterer Administratorkarten (nur Access Series FIPS)“ auf Seite 460.)
- **Verschlüsselte Daten** – Verschlüsselte Hostdaten in einer Access Series FIPS-Umgebung enthalten Schlüssel und andere Daten, die für die sichere Freigabe von Informationen erforderlich sind.

Diese Elemente sind aufeinander abgestimmt, um eine umfassende Security World zu erstellen. Beim Starten der Appliance wird die Gültigkeit der Security World überprüft und ermittelt, ob sich das Kryptographiemodul im Operationsmodus befindet, bevor der normale Betrieb aufgenommen wird.

Sie können das Kryptographiemodul mithilfe eines am Modul befindlichen Hardwareschalters in den Operationsmodus schalten. Es gibt folgende Schaltereinstellungen:

- **I** – Initialisierungsmodus. Verwenden Sie diese Einstellung, um das Kryptographiemodul mit einer neuen Security World zu initialisieren oder um ein Modul zu einer bestehenden Security World in einem IVE-Cluster hinzuzufügen.
- **O** – Operationsmodus. Mit dieser Einstellung können Sie das Kryptographiemodul nach der Initialisierung in den Operationsmodus versetzen. Beachten Sie, dass Sie den Schalter vor dem Einschalten des Moduls auf **O** setzen müssen, damit das Gerät mit der Routineverarbeitung beginnt. Andernfalls müssen Sie an der seriellen Konsole angeben, ob Sie sich mit der vorhandenen Security World verbinden oder eine neue initialisieren möchten.
- **M** – Wartungsmodus (engl. Maintenance). In künftigen Versionen kann die Firmware auf dem Kryptographiemodul mit dieser Einstellung aktualisiert werden. (Bisher nicht unterstützt.)

Weitere Informationen zum Initialisieren des Moduls und Erstellen einer neuen Security World finden Sie in der Kurzanleitung für NetScreen Access Series FIPS, die dem Produkt beiliegt.

Erstellen von Administratorkarten

Im Lieferumfang des Access Series FIPS sind sechs Smartcards enthalten. Eine ***Smartcard*** ist ein transportabler Schlüssel, der für den Zugriff auf zentrale Daten und Prozesse erforderlich ist, die vom Kryptographiemodul gesteuert werden. Bei der Initialisierung des Kryptographiemoduls über die serielle Konsole werden Sie von Access Series FIPS zunächst dazu aufgefordert, eine Smartcard zu verwenden. Während dieses Vorgangs erstellt Access Series FIPS eine Security World und wandelt die Smartcard in eine ***Administratorkarte*** um, die dem Karteninhaber exklusiven Zugriff auf die Security World gewährt.

Die Administratorkarte wird nur zum Initialisieren des Moduls benötigt. Für den normalen IVE-Betrieb nach der Initialisierung ist sie nicht erforderlich. Die Administratorkarte ist zum Durchführen der folgenden Aktionen erforderlich:

- Hinzufügen eines weiteren Access Series FIPS-Geräts zu einem Cluster (siehe „Hinzufügen eines IVE zu einem Cluster über die Webkonsole“ auf Seite 176)
- Neuinitialisieren eines Moduls mit einer neuen oder einer anderen Security World (Seite 461)
- Erstellen weiterer Administratorkarten (Seite 460)

Als Faustregel gilt, dass für jede Access Series FIPS-Operation, die über die serielle Konsole ausgeführt werden muss, eine Administratorkarte erforderlich ist.

Hinweis: Bei jeder Änderung der Security World müssen Sie bestimmen, wie die vorhandenen Administratorkarten verwendet werden. Folgende Optionen stehen zur Verfügung:
– Sie richten die vorhandenen Administratorkarten für die neue Security World neu ein.
– Sie verwenden Administratorkarten, die für die neue Security World vorinitialisiert sind und lassen die vorhandenen Administratorkarten unverändert. Beachten Sie aber, dass Sie bei dieser Option die alten, nicht geänderten Karten nicht zum Zugriff auf die neue Security World verwendet werden können.

Da Administratorkarten für Access Series FIPS-Operationen und die Sicherheit innerhalb Ihrer Security World von entscheidender Bedeutung sind, werden folgende Sicherheitsmaßnahmen dringend empfohlen:

- **Erstellen mehrerer Administratorkarten**.

  Sie können Administratorkarten nur ersetzen, wenn Sie eine andere gültige Karte besitzen und das Kennwort für den Kartensatz kennen. Das Kryptographiemodul speichert keine Wiederherstellungsdaten für Administratorkarten. Daher wird dringend empfohlen, dass Sie mindestens eine Administratorkarte für die Durchführung administrativer Standardaufgaben und eine weitere als Ersatz erstellen. Andernfalls laufen Sie Gefahr, Ihre einzige Administratorkarte und damit den Zugriff auf Ihre Security World und alle darin gespeicherten Daten zu verlieren.

- **Aufbewahren einer Ersatzadministratorkarte an einem sicheren Ort**.

  Bewahren Sie Ihre Ersatzadministratorkarten an einem sicheren Ort und nicht zusammen mit der Karte auf, die Sie für die täglichen Verwaltungsaufgaben verwenden, damit nicht alle Administratorkarten auf einmal verloren gehen können (z.B. durch Feuer oder Diebstahl).

- **Überschreiben aller verbleibenden Administratorkarte im Falle des Verlusts eine Karte**.

  Bei Verlust oder Beschädigung einer Administratorkarte sollten Sie umgehend eine neue Security World erstellen und alle verbleibenden Karten der alten Security World überschreiben. Andernfalls kann ein Angreifer mit einer alten Administratorkarte u.U. auf die alten Hostdaten auf einem Sicherungsband oder einem anderen Host zugreifen. Mit den alten Hostdaten und einer Karte ist der Angreifer dann vielleicht in der Lage, neue Schlüssel zu erstellen.

- **Schützen des Kennwortes einer Administratorkarte**.

  Sie sollten Ihr Kennwort aus Sicherheitsgründen niemals notieren oder nicht vertrauenswürdigen Benutzern mitteilen. Verwenden Sie auch keine Kennwörter, die einfach zu erraten sind. Die Sicherheit Ihres Kennwortes erhöht die Sicherheit der von Ihnen durchgeführten Operationen.

- **Verwenden Sie nur Administratorkarten aus bekannten und vertrauenswürdigen Quellen**.

  Verwenden Sie nur Smartcards aus vertrauenswürdigen Quellen, legen Sie Smartcards nie in nicht vertrauenswürdige Smartcardleser ein, und legen Sie keine nicht vertrauenswürdigen Smartcards in Ihren Smartcardleser ein.

Secure Meeting – Übersicht

Mit Secure Meeting können IVE-Benutzer Onlinekonferenzen sicher planen und durchführen, an denen sowohl IVE-Benutzer als auch Nicht-IVE-Benutzer teilnehmen können. Während einer Konferenz kann ein Benutzer seinen Desktop und seine Anwendungen über eine sichere Verbindung freigeben, sodass seine elektronischen Daten umgehend auch auf den Bildschirmen der anderen Teilnehmer vorliegen. Über die Desktop-Remotesteuerung und Textchats, die in einem eigenen, von der Vorführung unabhängigem Fenster erfolgen, können die Konferenzteilnehmer auch sicher online zusammenarbeiten. NetScreen bietet Secure Meeting auf zwei verschiedenen Appliances an:

- **Meeting Series-Appliance** – Die Meeting Series-Appliance ist ein dedizierter Konferenzserver für Umgebungen, in denen häufig Konferenzen abgehalten werden.
- **Access Series-Appliance mit Secure Meeting-Aktualisierung** – Die Secure Meeting-Aktualisierung ist auf Benutzer der Ascess Series zugeschnitten, die nur in begrenztem Umfang Konferenzen durchführen. Bei dieser Option vermittelt der Server, auf dem die Konferenzen durchgeführt werden, auch Anforderungen zwischen dem öffentlichen Internet und den internen Unternehmensressourcen.

Der Konfigurationsprozess für Meeting Series- und Access Series-Administratoren ist fast identisch, da beide Appliances auf der IVE-Plattform aufbauen. Für die wenigen Fälle, in denen die Verwaltungsaufgaben abweichen, enthält dieses Handbuch die entsprechenden Anweisungen für Access Series- und -Meeting Series-Administratoren.

Eine Übersicht über die Funktionen und Systemanforderungen von Secure Meeting finden Sie unter:

Konferenzplanung, -teilnahme und -durchführung 14
Zugriff auf den Konferenz-URL 17
Von Secure Meeting unterstützte Umgebungen 18

Konfigurationsanweisungen finden Sie unter Secure Meeting.

Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen 318
Konfigurieren der Seite „Meetings“ 375
Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle) . 157

Anweisungen für die Überwachung und Fehlerbehebung von Secure Meeting finden Sie unter:

(Nur Meeting Series-Appliances)
Anzeigen der Auslastung der Systemkapazität 126
Anzeigen und Absagen geplanter Konferenzen 133
Secure Meeting – Fehlerbehebung 20

Hinweis: Die hier aufgeführten Anweisungen ergänzen die Standard-Konfigurationsanweisungen für das IVE, die in diesem Handbuch aufgeführt sind.

Konferenzplanung, -teilnahme und -durchführung

Konferenzplanung

Jede Secure Meeting-Onlinekonferenz muss durch einen IVE-Benutzer geplant werden. Über die sichere Gatewayschnittstelle stellt der ***Ersteller der Konferenz*** die Konferenzdetails bereit, einschließlich Konferenzname, Beschreibung, Startzeit, Startdatum, Dauer, Kennwort, Teilnehmerliste und E-Mail-Adressen der Teilnehmer. Wenn der Ersteller der Konferenz die einzuladenden Personen angibt, muss er jeden ***Gast*** in eine der folgenden Kategorien einordnen:

- **IVE-Gast** – Ein IVE-Gast (auch als netzinterner Gast bezeichnet) ist ein IVE-Benutzer, der sich an demselben Server wie der Ersteller der Konferenz anmeldet.
- **Nicht-IVE Gast** – Ein Nicht-IVE-Gast (auch als netzexterner Gast bezeichnet) ist ein Nicht-IVE-Benutzer oder ein IVE-Benutzer, der sich über ein anderes IVE als das IVE[1] des Konferenzerstellers authentifiziert.

Wenn der Konferenzersteller die Konferenz speichert, fügt Secure Meeting die Konferenz auf der Seite **Meeting** hinzu. Die Seite wird allen IVE-Gästen (einschließlich des Konferenzerstellers) hinzugefügt, für die Sie die Seite **Meeting** aktiviert haben. Wenn Sie einen SMTP-Mailserver (Simple Mail Transfer Protocol) aktivieren, sendet Secure Meeting außerdem eine Benachrichtigungs-E-Mail an alle Gäste mit einer bekannten E-Mail-Adresse. Secure Meeting ruft die E-Mail-Adressen aus zwei Quellen ab:

- **Seite „Preferences"** – Ein IVE-Benutzer kann seine E-Mail-Adresse auf der Seite **Preferences** auf der IVE-Startseite angeben. Die Adresse wird

1. Secure Meeting gewährleistet zwar, dass Nicht-IVE-Gäste bei der Anmeldung ihren Namen eingeben müssen, die Namen werden jedoch nicht authentifiziert. Zur Authentifizierung von Nicht-IVE-Gästen verwendet Secure Meeting nur die Konferenz-IDs und Kennwörter.

dann automatisch verwendet, wenn dieser Teilnehmer zu einer Konferenz eingeladen wird.

- **Seite „Create Meeting"** – Der Konferenzersteller kann die E-Mail-Adressen von Konferenzteilnehmern manuell eingeben (oder überschreiben), wenn er eine Konferenz plant oder aktualisiert.

Die E-Mail-Nachricht enthält Konferenzdetails und eine Verknüpfung, über die der Gast der Konferenz beitreten kann. Teilnehmer können einer Konferenz bis 15 Minuten vor ihrem Start beitreten. (Weitere Informationen finden Sie unter „Zugriff auf den Konferenz-URL" auf Seite 17.)

Erstellen von Sofortkonferenzen

Durch Erstellung einer ***Sofortkonferenz*** kann die Konferenzplanung erheblich abgekürzt werden. Wenn der IVE-Benutzer auf **Instant Meeting** klickt, erstellt Secure Meeting automatisch eine Konferenz mit einem eindeutigen Namen und Kennwort, legt den Beginn der Konferenz auf sofort fest, gibt eine Dauer von 30 Minuten an, fügt den Konferenzersteller als einzigen Teilnehmer hinzu und zeigt die Seite **Launch Meeting Application** auf dem Desktop des Konferenzerstellers an. Auf dieser Seite aus kann der Konferenzersteller das automatisch erstellte Kennwort ändern oder annehmen und die Konferenz starten.

Da der Konferenzersteller der einzige Teilnehmer der Sofortkonferenz ist, kann er andere Teilnehmer nicht mithilfe von E-Mail-Benachrichtigungen hinzufügen. Stattdessen muss er anderen Teilnehmern die für die Konferenzteilnahme erforderlichen Informationen zusenden, z. B. URL, ID und Kennwort. Diese Informationen werden auf der Seite **Launch Meeting Application** angegeben.

Da der Konferenzersteller auch der einzige IVE-Teilnehmer ist, kann er als Einziger die Konferenz leiten.

Konferenzteilnahme

Wenn der Gast der Konferenz beitritt, lädt Secure Meeting eine ActiveX-Komponente oder ein Java-Applet auf das System des Gastes herunter. Die Clientkomponente enthält einen Konferenz-Betrachter, Präsentationstools und eine Anwendung zur Übermittlung von Textnachrichten. Nachdem Secure Meeting die ActiveX-Komponente oder das Java-Applet auf dem Desktop des Benutzers gestartet hat, wird der Benutzer zum ***Konferenzteilnehmer*** und kann sich an der Konferenz beteiligen. (Informationen über das von Secure Meeting heruntergeladene ActiveX-Steuerelement bzw. Java-Applet finden Sie unter „Von Secure Meeting unterstützte Umgebungen" auf Seite 18.)

Sobald ein Teilnehmer einer Konferenz beigetreten ist, kann er im Fenster **Secure Meeting Chat** Textnachrichten an andere Teilnehmer senden.

Konferenzdurchführung

Der ***Konferenzleiter*** ist für das Starten der Konferenz verantwortlich und muss einen Vorführenden benennen. Solange er einer Konferenz nicht beigetreten ist, können die anderen Teilnehmer nur chatten. Sie können keine Vorführung anzeigen oder durchführen, weil der Konferenzleiter standardmäßig auch gleichzeitig ***Vorführende*** ist. Er (oder ein von ihm ernannter Teilnehmer) startet die Konferenzvorführung, indem er seinen Desktop oder einige Anwendungen für die anderen Teilnehmer freigibt. Nach der Freigabe durch den Vorführenden wird auf dem Desktop jedes Konferenzteilnehmers automatisch ein Konferenz-Betrachter geöffnet, in dem die freigegebenen Anwendungen des Vorführenden[1] angezeigt werden.

Der Konferenzleiter kann Teilnehmer ggf. auch von der Konferenz ausschließen, die Konferenz verlängern, falls die geplante Dauer überschritten wird, und die Konferenz beenden. Der Konferenzleiter kann seine Verantwortlichkeiten während einer Konferenz auf einen anderen Teilnehmer übertragen. Dieser muss aber in der richtigen Umgebung arbeiten. Der Konferenzleiter kann jeden beliebigen IVE Benutzer als Konferenzleiter und jeden beliebigen Windows-Benutzer als Vorführenden einsetzen.

Der Vorführende kann auch Verantwortung an einen anderen Teilnehmer abgeben, indem er einen Steuernden bestimmt. Ein ***Steuernder*** verwendet seine eigene Maus und Tastatur zur Remotesteuerung des freigegebenen Desktops oder der freigegebenen Anwendungen des Vorführenden. Beachten Sie, dass der Vorführende die Berechtigung für die Remotesteuerung nicht nur IVE-Teilnehmern und Windows-Benutzern, sondern allen Teilnehmern erteilen kann. Wenn der Vorführende die Kontrolle über seine remote gesteuerten Anwendungen zurückerlangen möchte, muss er lediglich an einer beliebigen Stelle mit der rechten Maustaste klicken, um die Steuerung von Secure Meeting wieder zurückzuerhalten.

1. Secure Meeting kann den Inhalt des Desktops des Vorführenden nicht anzeigen, wenn er gesperrt ist.

Zugriff auf den Konferenz-URL

Für die Teilnahme an einer Konferenz müssen Secure Meeting-Teilnehmer über den Konferenz-URL zur Konferenzseite auf dem Secure Meeting-Server (IVE)[1] wechseln. Auf den URL kann ganz einfach zugegriffen werden:

- Sie können die Verknüpfung in der Benachrichtigungs-E-Mail verwenden.
- Sie können den URL auf der Seite **Launch Meeting application** eingeben.
- Sie können auf die Verknüpfung **Join Meeting** klicken, die in der Benutzersitzung über das sichere Gateway angezeigt wird (nur IVE-Gäste).

Der Gast kann den URL in folgendem Format zusammensetzen und dann in die Navigationsleiste des Browser eingeben:

```
https://IhrIVE/Meeting/KonferenzID
```

Dabei gilt:

- `IhrIVE` ist der Name und die Domäne des IVE, auf dem die Konferenz stattfindet, z.B. `iveserver.firmenname.com`. Dieser Name wird aus dem Feld **Virtual Hostname** auf der Registerkarte **System > Network > Internal Port** übernommen, sofern er dort angegeben wurde. Andernfalls verwendet Secure Meeting beim Erstellen des Konferenz-URLs den IVE-Namen aus dem Browser des Konferenzerstellers.
- `Meeting` ist eine Literalzeichenfolge. (Beachten Sie, dass diese Zeichenfolge nicht verändert wird.)
- `KonferenzID` ist die eindeutige Kennnummer aus 8 Ziffern, die für diese Konferenz generiert wurde (optional). Wenn der Benutzer die ID nicht in den URL einfügt, wird er bei der Konferenzanmeldung zur Eingabe des URL aufgefordert.

Beispiel:

```
https://connect.acmegizmo.com/Meeting/86329712
```

1. Secure Meeting hält Onlinekonferenzen auf dem NetScreen Instant Virtual Extranet ab, an denen sowohl IVE-Benutzer als auch Nicht-IVE-Benutzer teilnehmen können. Nicht-IVE-Konferenzteilnehmer können im IVE jedoch ausschließlich auf die Konferenz zugreifen, zu der sie eingeladen wurden.

Von Secure Meeting unterstützte Umgebungen

Secure Meeting kann in den unterschiedlichsten Umgebungen eingesetzt werden. Je nach Systemkonfiguration arbeitet Secure Meeting möglicherweise unterschiedlich und stellt andere Funktionsebenen bereit. Dies wird in den folgenden Abschnitten beschrieben.

Mit der Secure Meeting-Kompatibilitätsüberprüfung können Sie am einfachsten feststellen, ob Ihr System mit Secure Meeting kompatibel ist. Wechseln Sie hierfür mithilfe des Konferenz-URL (`https://IhrIVE/Meeting`) zur Konferenzanmeldeseite, und klicken Sie auf **Konferenzkompatibilität überprüfen**. Secure Meeting ermittelt den Grad der Kompatibilität und schlägt zum Erreichen voller Kompatibilität ggf. Aktualisierungen vor. Nach der Planung einer Konferenz können Sie jederzeit die Kompatibilitätsüberprüfung ausführen. Sie müssen damit nicht bis zum Beginn der Konferenz warten.

Wichtig: Die Kompatibilitätsüberprüfung von Secure Meeting überprüft nicht die Verbindungsgeschwindigkeit, den Legacymodus und weitere Faktoren, die eine Konferenz beeinflussen können. Informationen zu Faktoren, die nicht überprüft werden, finden Sie unter „Weitere Systemanforderungen und Einschränkungen“ auf Seite 19.

Betriebssystem- und Browseranforderungen

Secure Meeting wird von unterschiedlichen Betriebssystemen in verschiedenem Umfang unterstützt. Ausführung von Secure Meeting unter folgenden Betriebssystemen:

- **Windows-Betriebssystem** – Sie können auf alle Konferenzfunktionen zugreifen. Zu den unterstützten Betriebssystemen von Windows gehören Windows 98 SE, Windows ME, Windows 2000 mit Service Pack 4, Windows NT 4.0 mit Service Pack 6 und Windows XP mit Service Pack 1. Zu den unterstützten Browsern auf Betriebssystemen von Windows gehören Internet Explorer 6.0 mit Service Pack 1 und Netscape Navigator 7.1. Mit Ausnahme von Windows XP werden unter allen oben genannten Betriebssystemen von Windows Internet Explorer 5.0 und 5.5 mit Service Pack 2 unterstützt.
- **Andere Betriebssysteme als Windows** – Konferenzen können angezeigt, geleitet oder remote gesteuert, jedoch nicht vorgeführt werden. Secure Meeting kann theoretisch unter jedem Betriebssystem ausgeführt werden, wenn die entsprechende Java Virtual Machine (JVM) auf

diesem installiert ist. In Umgebungen, die nicht unter Windows laufen, wird jedoch empfohlen, Mac OS X 10.3 mit Safari 1.1.1 oder Linux Redhat 7.3 mit Mozilla 1.1 zu verwenden.

Zusätzlich zu den oben genannten Browseranforderungen müssen im Browser JavaScript und eine der folgenden Komponenten[1] installiert sein:

- **ActiveX-Komponenten** – ActiveX-Steuerelemente werden für Administratoren und Hauptbenutzer in Windows 2000-Systemen automatisch aktiviert, Standardbenutzer müssen sie hingegen manuell aktivieren. Um ActiveX-Steuerelemente in Internet Explorer* zu aktivieren, wählen Sie **Extras > Internetoptionen > Sicherheit > Stufe anpassen** aus, und aktivieren Sie anschließend im Dialogfeld **Sicherheitseinstellungen** die ActiveX-Komponenten.
- **Microsoft Java Virtual Machine (JVM)** – Um Microsoft JVM in Internet Explorer* zu aktivieren, wählen Sie **Extras > Internetoptionen > Sicherheit > Stufe anpassen** aus, und aktivieren Sie dann im Dialogfeld **Security Settings** die Option **Microsoft VM**.
- **Sun Java Virtual Machine (JVM) 1.4 .1_01 oder höher –** Secure Meeting führt ein Java-Applet im Arbeitsspeicher aus, wenn Sie einer Konferenz beitreten. Secure Meeting wird von den Sun JVM-Versionen 1.4.1_01 und höher unterstützt. Sun JVM kann unter der Adresse www.java.com heruntergeladen werden.

So aktivieren Sie JavaScript:

- **Internet Explorer*** – Navigieren Sie zur Registerkarte **Extras > Internetoptionen > Sicherheit**, und wählen Sie **Stufe anpassen** aus. Wählen Sie unter **Scripting von Java-Applets** die Option **Aktivieren** aus.
- **Netscape Navigator*** – Wechseln Sie zu **Bearbeiten > Einstellungen**. Aktivieren Sie unter **Erweitert> Scripts & Plugins** das Kontrollkästchen **Navigator**.

* Die Anweisungen beziehen sich auf die neuesten Browserversionen. Die Anweisungen für ältere Browser können davon abweichen.

Weitere Systemanforderungen und Einschränkungen

Secure Meeting unterstützt das Abhalten von Konferenzen mit 16-Bit- oder 32-Bit-Farbanzeige auf dem Bildschirm. Secure Meeting wird *nicht* in IVE-Umgebungen unterstützt, die mit dem 2.x-Autorisierungsmodus des IVE

1. Wenn im Browser ActiveX-Komponenten aktiviert sind, lädt Secure Meeting eine ActiveX-Komponente auf den Clientcomputer herunter, wenn Sie einer Konferenz beitreten. Wenn hingegen eine JVM installiert ist, lädt Secure Meeting ein Java-Applet herunter, wenn Sie einer Konferenz beitreten.

konfiguriert sind (Legacymodus). Sie können mit Secure Meeting keine Streamingmedien-Anwendungen freigeben. Diese Einschränkungen gelten zusätzlich zu den Einschränkungen in der Lizenz.

Wenn Sie Secure Meeting mit einem SSL-Zertifikat verwenden, empfiehlt es sich, auf Produktionsebene ein Zertifikat auf dem Secure Meeting-Server (d.h. dem IVE) zu installieren. Wenn Sie ein selbst signiertes SSL-Zertifikat installieren, können für Secure Meeting-Benutzer möglicherweise Schwierigkeiten bei der Konferenzanmeldung auftreten (siehe „Serverzertifikate" auf Seite 69). Wenn Sie ein selbst signiertes Zertifikat verwenden möchten, weisen Sie die Konferenzteilnehmer an, das Zertifikat vor dem Beitreten der Konferenz zu installieren. (In Internet Explorer klicken die Benutzer auf **Zertifikat anzeigen** und dann auf **Zertifikat installieren**, wenn die Fehlermeldung angezeigt wird.)

Secure Meeting – Fehlerbehebung

Wenn mit Secure Meeting Probleme auftreten, empfehlen wir Folgendes:

- **Deinstallieren Sie den Secure Meeting-Client von Ihrem System**.

  Wenn beim Starten von Secure Meeting ein Problem auftritt, klicken Sie auf die Verknüpfung **Joining a Meeting: Troubleshooting** auf der Seite **Launch Meeting Application**. Klicken Sie dann auf **Uninstall**. Klicken Sie auf **Return to Meeting** und versuchen Sie erneut, die Konferenz zu starten. Beim nächsten Versuch, einer Konferenz beizutreten, aktualisiert Secure Meeting Ihren Client mit der aktuellen Version.

- **Weitere Informationen können Sie der PDF-Datei Secure Meeting Error Messages** entnehmen.

  In der PDF-Datei *Secure Meeting Error Messages* sind Fehler aufgeführt, die beim Konfigurieren oder Verwenden von Secure Meeting auftreten können, und wird der Umgang mit diesen Fehlern erläutert. Die PDF-Datei ist verfügbar auf unserer Supportsite: www.support.netscreen.com.

- **Kontaktaufnahme mit dem NetScreen-Support**

  Wenn ein Fehler auftritt, den Sie mit den oben beschriebenen Verfahren nicht beheben können, senden Sie eine klare Beschreibung des Problems an den NetScreen-Support. Geben Sie detailliert an, wie der Fehler und der Fehlermeldungstext nachzuvollziehen sind, und geben Sie Ihr IVE-Betriebssystem mit Buildnummer und Ihre IVE-Administratorprotokolldateien, Installationsprotokolldateien und Clientprotokolldateien an.

Zugriff auf Clientprotokolldateien

Je nach den Rechten des Betriebssystems installiert Secure Meeting Clientdateien in unterschiedlichen Verzeichnissen. Folgende Browseroptionen sind möglich:

- **Power user or administrative privileges on a Windows system**

  Secure Meeting installiert Dateien im Verzeichnis **C:\Programme\Neoteris\Secure Meeting <Versionsnummer>\ dsCboxUI.log**.

- **Regular user privileges on a Windows system**

  Secure Meeting installiert Dateien im Verzeichnis **C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Temp\ dsCboxUI.log** oder unter **C:\dsCboxUI.log**.
  Wenn Sie die Protokolldateien nicht im ersten Verzeichnis finden, müssen Sie ggf. die Anzeige von versteckten Dateien und Ordnern aktivieren. (Wählen Sie in Windows Explorer im Menü **Extras** die Option **Ordneroptionen** aus. Aktivieren Sie auf der Registerkarte **Ansicht** die Option **Alle Dateien und Ordner anzeigen**, und klicken Sie anschließend auf **OK**.)

- **Andere Systeme als Windows**

  Secure Meeting schreibt in die Java-Konsole. Kopieren Sie den Inhalt der Java-Konsole, und fügen Sie ihn in eine Datei ein, die Sie an den NetScreen-Support senden können.

Zugriff auf Installationsprotokolle

Wenn Secure Meeting in einer Windows-Umgebung ausgeführt wird, suchen Sie die Installationsprotokolle in folgenden Verzeichnissen:

- **C:\WINNT\Übertragene Programmdateien\NeoterisSetup.log**
- **C:\NeoterisSetup.log**

Wenn Secure Meeting in einer anderen Umgebung als unter Windows ausgeführt wird, schreibt es in die Java-Konsole. Kopieren Sie den Inhalt der Java-Konsole, und fügen Sie ihn in eine Datei ein, die Sie an den NetScreen-Support senden können.

Zugriff auf Administratorprotokolle

Administratorprotokolle sind in der Webkonsole auf der Seite **System > Log/Monitoring** zu finden. Beachten Sie dabei, dass es drei Protokolle gibt: Ereignisprotokoll (Events Log), Benutzerzugriffsprotokoll (User Access Log) und Administratorzugriffsprotokoll (Administrator Access Log).

Zugriffsverwaltung – Übersicht

Das IVE ermöglicht Ihnen, die Ressourcen Ihres Unternehmens mithilfe von Authentifizierungsrichtlinien, Benutzerprofilen und Ressourcenrichtlinien zu sichern. Mit diesen drei Kontrollstufen können Sie die Zugriffsverwaltung für das gesamte Unternehmen steuern. Sie können Sicherheitsanforderungen angeben, die Benutzer erfüllen müssen, um sich beim IVE anzumelden und auf IVE-Funktionen oder bestimmte URLs, Dateien und weitere Serverressourcen zugreifen zu können. Das IVE setzt die konfigurierten Richtlinien, Regeln und Einschränkungen sowie die Bedingungen durch, mit deren Hilfe die Benutzer daran gehindert werden, Verbindungen mit unautorisierten Ressourcen und Inhalten herzustellen oder diese herunterzuladen.

Weitere Informationen finden Sie unter:

Richtlinien, Regeln und Einschränkungen sowie Bedingungen 23
Angeben von Sicherheitsanforderungen 26

Richtlinien, Regeln und Einschränkungen sowie Bedingungen

Der Zugriff auf Ressourcen beginnt im Authentifizierungsbereich. Als ***Authentifizierungsbereich*** wird eine Gruppierung von Authentifizierungsressourcen bezeichnet. Dies umfasst:

- **Ein Authentifizierungsserver**, der die Identität des Benutzers überprüft und bestätigt. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter (Seite 212).
- **Eine Authentifizierungsrichtlinie**, die die Sicherheitsanforderungen des Bereichs angibt, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet (Seite 203).
- **Ein Verzeichnisserver** ist ein LDAP-Server, der dem IVE Benutzer- und Gruppeninformationen bereitstellt, mit denen das IVE Benutzer zu einer oder mehreren Benutzerrollen zuordnet (Seite 229).
- **Rollenzuordnungsregeln** geben die Bedingungen an, die ein Benutzer erfüllen muss, damit ihn das IVE zu einer oder mehreren Rollen zuweist. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers (Seite 277).

Einer IVE-Anmeldeseite sind ein oder mehrere Authentifizierungsbereiche zugeordnet. Wenn mehrere Bereiche für eine Anmeldeseite vorhanden sind, muss der Benutzer vor der Übermittlung der Anmeldeinformationen einen Bereich angeben. Wenn der Benutzer die Anmeldeinformationen übermittelt hat, überprüft das IVE die Authentifizierungsrichtlinie des gewählten Bereichs. Der Benutzer muss die für die Authentifizierungsrichtlinien des Bereichs angegebenen Sicherheitsanforderungen erfüllen, andernfalls leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter.

Sie können auf Bereichsebene Sicherheitsanforderungen angeben, die auf folgenden Aspekten basieren: der Quell-IP des Benutzers, dem Browser, von dem aus der Zugriff auf das IVE erfolgt, der Besitz eines clientseitigen Zertifikates, die Länge des Benutzer-Kennwortes, ob die Hostprüfung installiert ist, oder ob die Cachebereinigung auf dem Benutzercomputer installiert ist oder ausgeführt wird. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wurde, wertet das IVE die Rollenzuordnungsregeln für den Bereich aus und ermittelt, welche Rollen dem Benutzer zugeordnet werden.

Eine ***Rolle*** ist eine definierte Einheit, die die IVE-Sitzungseigenschaften für die Benutzer angibt, die der Rolle zugeordnet sind. Diese Sitzungseigenschaften enthalten Informationen wie Sitzungszeitbegrenzungen, Lesezeichen und aktivierte Zugriffsfunktionen – Webbrowsing, Dateinavigation, Secure Application Manager, Telnet/SSH, Network Connect, Secure Meeting und E-Mail-Client. Die Rollenkonfiguration bildet die zweite Ebene der Ressourcenzugriffssteuerung. Eine Rolle gibt nicht nur die Zugriffsmechanismen an, die einem Benutzer zur Verfügung stehen, sondern auch Beschränkungen, denen Benutzer entsprechen müssen, um einer Rolle zugeordnet werden zu können. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls ordnet ihn das IVE keiner Rolle zu.

Auf Rollenebene können Sie Sicherheitsanforderungen auf der Grundlage folgender Aspekte angeben: Quell-IP des Benutzers, Browser, Besitz eines clientseitigen Zertifikats, ob die Hostprüfung installiert ist oder bestimmte Richtlinien auf dem Benutzercomputer durchsetzt und ob die Cachebereinigung auf dem Benutzercomputer ausgeführt wird. Wenn der Benutzer die Anforderungen erfüllt, die von einer Rollenzuordnungsregel oder den Einschränkungen einer Rolle[1] angegeben sind, ordnet das IVE den Benutzer zu

1. Sicherheitsanforderungen für eine Rolle können an zwei Positionen angegeben werden: in den Rollenzuordnungsregeln eines Authentifizierungsbereichs (mit benutzerdefinierten Ausdrücken) oder durch die Angabe von Einschränkungen in der Rollendefinition. Das IVE wertet die angegebenen Anforderungen an beiden Positionen aus. Dies gewährleistet, dass nur Benutzer einer Rolle zugeordnet werden, die die Anforderungen erfüllen.

einer Rolle zu. Wenn ein Benutzer eine Anforderung an die für die Rolle verfügbaren Backend-Ressourcen sendet, wertet das IVE die entsprechenden Ressourcenrichtlinien für die Zugriffsfunktion aus.

Eine ***Ressourcenrichtlinie*** ist eine Reihe von Ressourcennamen (wie URLs, Hostnamen und Kombinationen aus IP-Adresse und Netzmaske), denen der Zugriff oder die Ausführung anderer ressourcenspezifischer Aktionen wie Neuschreiben oder Zwischenspeicherung gewährt oder verweigert wird. Eine Ressourcenrichtlinie bildet die dritte Ebene der Ressourcenzugriffssteuerung. Eine Rolle gewährt den Zugriff auf bestimmte Funktionen und Ressourcen (wie Lesezeichen und Anwendungen), wohingegen eine Ressourcenrichtlinie den Benutzerzugriff auf eine bestimmte Ressourcen steuert. Mithilfe dieser Richtlinien können sogar Bedingungen angegeben werden, die, sofern erfüllt, den Benutzerzugriff auf eine Serverfreigabe oder Datei verweigern oder gewähren. Derartige Bedingungen können auf den von Ihnen angegebenen Sicherheitsanforderungen basieren. Der Benutzer muss diese Sicherheitsanforderungen erfüllen, andernfalls wird die Benutzeranforderung vom IVE nicht verarbeitet.

Auf Ressourcenebene können Sie Sicherheitsanforderungen auf der Grundlage folgender Aspekte angeben: Quell-IP des Benutzers, Browser, Besitz eines clientseitigen Zertifikats, Tageszeit der Anforderung, ob die Hostprüfung installiert ist oder bestimmte Richtlinien auf dem Benutzercomputer durchsetzt und ob die Cachebereinigung auf dem Benutzercomputer installiert ist oder ausgeführt wird. Wenn der Benutzer die Anforderungen erfüllt, die in den Bedingungen einer Ressourcenrichtlinie angegeben sind, verweigert oder gewährt das IVE den Zugriff auf die angeforderte Ressource. Sie können z. B. Webzugriff auf Rollenebene aktivieren, sodass ein der Rolle zugewiesener Benutzer eine Webanforderung ausführen kann. Sie können auch eine Webressourcenrichtlinie so konfigurieren, dass Anforderungen an einen bestimmten URL oder Pfad verweigert werden, wenn die Hostprüfung auf dem Benutzercomputer eine inakzeptable Datei findet. In diesem Szenario überprüft das IVE, ob die Hostprüfung ausgeführt wird und gibt dann an, dass der Benutzercomputer der erforderlichen Hostprüfung-Richtlinie entspricht. Wenn dies der Fall ist, d. h. die inakzeptable Datei nicht gefunden wurde, gewährt das IVE dem Benutzer Zugriff auf die angeforderte Webressource.

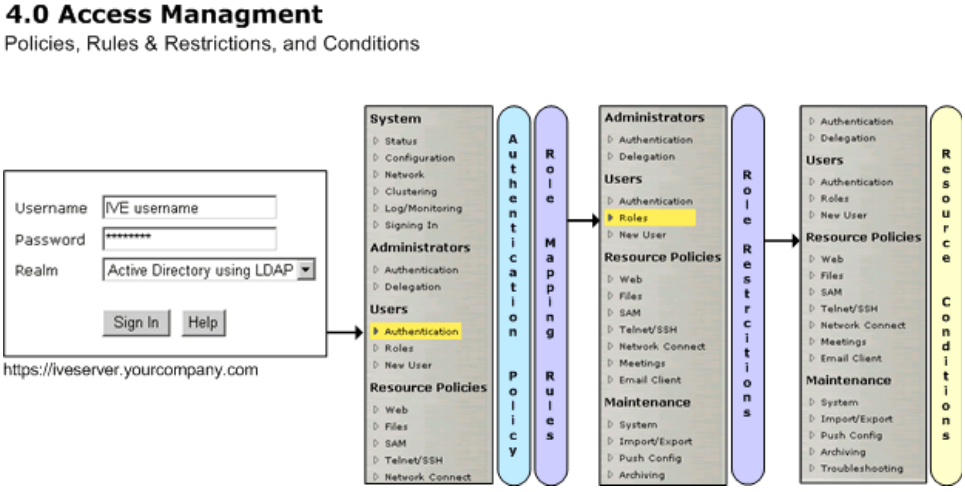


Abbildung 2:Zugriffsverwaltung
In dieser Abbildung ist die Reihenfolge dargestellt, in der das IVE Richtlinien, Regeln, Einschränkungen und Bedingungen auswertet, nachdem ein Benutzer seine Anmeldeinformationen auf der Anmeldeseite übermittelt hat.

Angeben von Sicherheitsanforderungen

Mit dem IVE können Sicherheitsanforderungen für Administratoren und Benutzer ganz einfach über die folgenden Optionen und Funktionen angegeben werden:

Quell-IP 26
Browser 28
Zertifikat 29
Kennwort 30
Hostprüfung 31
Cachebereinigung 32

Quell-IP

Sie können den Zugriff auf das IVE und die Ressourcen anhand der Quell-IP einschränken.

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, dessen Kombination aus IP-Adresse und Netzmaske den angegebenen Quell-IP-Anfor-

derungen für den ausgewählten Authentifizierungsbereich entspricht. Verfügt der Benutzercomputer nicht über eine für den Bereich erforderliche Kombination aus IP-Adresse und Netzmaske, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP

Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, dessen Kombination aus IP-Adresse und Netzmaske den angegebenen Quell-IP-Anforderungen für jede der Rollen entspricht, zu denen das IVE den Benutzer zuordnet. Verfügt der Benutzercomputer nicht über eine Kombination aus IP-Adresse und Netzmaske, die für eine Rolle erforderlich ist, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Source IP

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte*|*erstellte Regel* > *Benutzerdefinierter Ausdruck*

  oder so: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Source IP

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Computer durchführen, dessen Kombination aus IP-Adresse und Netzmaske den im Zusammenhang mit der Benutzeranforderung angegebenen Quell-IP-Anforderungen für die Ressourcenrichtlinie entspricht. Verfügt der Benutzercomputer nicht über die erforderliche Kombination aus IP-Adresse und Netzmaske, die für eine Ressource erforderlich ist, gewährt das IVE dem Benutzer keinen Zugriff auf die Ressource.

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Browser

Sie können den Zugriff auf das IVE und auf Ressourcen anhand des Browsertyps einschränken.

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Browser anmelden, dessen Benutzer-Agent-Zeichenfolge dem Zeichenfolgenmuster entspricht, das für den ausgewählten Authentifizierungsbereich angegeben wurde. Wenn die Benutzer-Agent-Zeichenfolge des Browsers für den Bereich zulässig ist, leitet das IVE die Anmeldeinformationen an den Authentifizierungsserver weiter. Wenn die Benutzer-Agent-Zeichenfolge des Browsers nicht für den Bereich zulässig ist, leitet das IVE die Anmeldeinformationen nicht an den Authentifizierungsserver weiter.

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Browser anmelden, dessen Benutzer-Agent-Zeichenfolge den jeweils angegebenen Zeichenfolgenmustern für die einzelnen Rollen entspricht, denen der Benutzer durch das IVE zugeordnet werden kann. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Rolle entspricht, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Browser

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich*> Role Mapping > *Ausgewählte*|*Erstellte Regel* > *Benutzerdefinierter Ausdruck*

  oder so: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Browser

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Browser durchführen, dessen Benutzer-Agent-Zeichenfolge mit den Zulassungsanforderungen für die Ressourcenrichtlinie übereinstimmt, die für die Benutzeranforderung gilt. Wenn die Benutzer-Agent-Zeichenfolge nicht den Zulassungsanforderungen für eine Ressource entspricht, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Resource > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Zertifikat

Sie können den Zugriff auf das IVE und die Ressourcen durch Anforderung clientseitiger Zertifikate einschränken:

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer kann sich nur von einem Computer anmelden, der das angegebene clientseitige Zertifikat besitzt (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare). Wenn der Benutzercomputer die für den Bereich erforderlichen Zertifikatsinformationen nicht besitzt, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter.

  Die Stammzertifizierungsstelle, die zur Überprüfung der Clientzertifikate verwendet werden soll, wird folgendermaßen angegeben: System > Configuration > Certificates > CA Certificates

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für jede der Rollen erfüllt, zu der das IVE den Benutzer zuordnet. Besitzt der Benutzercomputer nicht die Zertifikatinformationen, die für eine Rolle erforderlich sind, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

  Die Stammzertifizierungsstelle, die zur Überprüfung der Clientzertifikate verwendet werden soll, wird folgendermaßen angegeben: System > Configuration > Certificates > CA Certificates

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Certificate

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte*|*erstellte Regel* > *Zertifikatattribut*|*Benutzerdefinierter Ausdruck*

Weitere Rollenanforderungen können folgendermaßen angegeben werden: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Certificate

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer muss eine Ressourcenanforderung von einem Computer ausführen, der die angegebenen Anforderungen des clientseitigen Zertifikats (von der richtigen Zertifizierungsstelle (CA) ausgestellt und mit optional angegebenen Anforderungen für Feld-Wert-Paare) für die Ressourcenrichtlinie erfüllt, die für die Benutzeranforderung angegeben wurde. Besitzt der Benutzercomputer nicht die Zertifikatsinformationen, die für eine Ressource erforderlich sind, verweigert das IVE dem Benutzer den Zugriff auf die Ressource.

  Die Stammzertifizierungsstelle, die zur Überprüfung der Clientzertifikate verwendet werden soll, wird folgendermaßen angegeben: System > Configuration > Certificates > CA Certificates

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Kennwort

Sie können den Zugriff auf das IVE und auf Ressourcen anhand der Kennwortlänge einschränken.

Bei Anmeldung von Administratoren oder Benutzern am IVE**.**

Der Benutzer muss ein Kennwort eingeben, das der Mindestkennwortlänge entspricht, die für den Bereich angegeben wurde. Beachten Sie, dass die Datensätze für lokale Benutzer und Administratoren auf dem IVE-Authentifizierungsserver gespeichert werden. Auf diesem Server müssen Kennwörter mindestens 6 Zeichen lang sein, unabhängig von dem Wert, der für die Authentifizierungsrichtlinie des Bereichs angegeben wurde.

Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

Hostprüfung

Sie können den Zugriff auf das IVE und die Ressourcen anhand der Quell-IP einschränken.

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Richtlinien entspricht, die für den Bereich angegeben wurden. Wenn der Benutzercomputer den Anforderungen der Hostprüfung-Richtlinien nicht entspricht, die für den Bereich angegeben wurden, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

  Systemweite Richtlinien für die Hostprüfung werden folgendermaßen angegeben: System > Configuration > Security > Hostprüfung

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Richtlinien für jede der Rollen entspricht, zu denen das IVE den Benutzer zuordnet. Wenn der Benutzercomputer die Anforderungen der Hostprüfung-Richtlinien nicht erfüllt, die für eine Rolle angegeben wurden, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

  Systemweite Richtlinien für die Hostprüfung werden folgendermaßen angegeben: System > Configuration > Security > Hostprüfung

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte*|*erstellte Regel* > *Benutzerdefinierter Ausdruck*

  Weitere Rollenanforderungen können folgendermaßen angegeben werden: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer kann eine Ressourcenanforderung nur von einem Computer ausführen, der den Hostprüfung-Richtlinien für die Ressourcenrichtlinie entspricht, die für die Benutzeranforderung gilt. Wenn der Benutzercomputer die Anforderungen der Hostprüfung-Richtlinien nicht erfüllt, die für eine Ressource angegeben wurden, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

Diese Sicherheitsanforderung kann von allen Benutzern folgendermaßen konfiguriert werden: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Cachebereinigung

Sie können den Zugriff auf das IVE und die Ressourcen durch Anforderung der Cachebereinigung einschränken:

- **Bei Anmeldung von Administratoren oder Benutzern am IVE**

  Der Benutzer muss sich von einem Computer anmelden, der den Richtlinien für die Cachebereinigung entspricht, die für den Bereich angegeben wurden. Wenn der Benutzercomputer den Anforderungen der Richtlinien für die Cachebereinigung nicht entspricht, die für den Bereich angegeben wurden, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und dem Benutzer wird der Zugriff auf das IVE verweigert.

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cachebereinigung

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cachebereinigung

- **Bei Zuordnung von Administratoren oder Benutzern zu einer Rolle**

  Der authentifizierte Benutzer muss sich von einem Computer anmelden, der der Anforderung für die Cachebereinigung entspricht, die für jede der Rollen angegeben wurde, zu der das IVE den Benutzer zuordnet. (Dabei muss die Cachebereinigung, je nach Konfiguration, auf der Arbeitsstation ausgeführt oder ggf. installiert werden.) Wenn der Benutzercomputer die Anforderungen für die Cachebereinigung, die für eine Rolle angegeben wurden, nicht erfüllt, ordnet das IVE den Benutzer nicht zu dieser Rolle zu.

  Administratoren konfigurieren diese Sicherheitsanforderung folgendermaßen: Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Cachebereinigung

  Benutzer konfigurieren diese Sicherheitsanforderung folgendermaßen: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Cachebereinigung

  Weitere Rollenanforderungen können folgendermaßen angegeben werden: Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Cachebereinigung

- **Bei Anforderung einer Ressource durch einen Benutzer**

  Der authentifizierte, autorisierte Benutzer muss sich von einem Computer anmelden, der der Anforderung an die Cachebereinigung für die

Ressourcenrichtlinien entspricht, die für die Anforderung des Benutzers gültig ist. (Dabei muss die Cachebereinigung, je nach Konfiguration, auf der Arbeitsstation ausgeführt oder ggf. installiert werden.) Wenn der Benutzercomputer die Anforderung an die Cachebereinigung nicht erfüllt, die für eine Ressource angegeben wurde, gewährt das IVE dem Benutzer keinen Zugriff auf die Ressource.

Diese Sicherheitsanforderung wird folgendermaßen konfiguriert: Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Authentifizierungsbereiche – Übersicht

Als ***Authentifizierungsbereich*** wird eine Gruppierung von Authentifizierungsressourcen bezeichnet. Dies umfasst:

- **Ein Authentifizierungsserver**, durch den die Identität des Benutzers überprüft wird. Das IVE leitet die Anmeldeinformationen eines Benutzers von der Anmeldeseite an einen Authentifizierungsserver weiter (Seite 35).
- **Eine Authentifizierungsrichtlinie**, die die Sicherheitsanforderungen des Bereichs angibt, die erfüllt sein müssen, damit das IVE die Anmeldeinformationen eines Benutzers zur Überprüfung an einen Authentifizierungsserver weiterleitet (Seite 36).
- **Ein Verzeichnisserver** ist ein LDAP-Server, der dem IVE Benutzer- und Gruppeninformationen bereitstellt, mit denen das IVE Benutzer zu einer oder mehreren Benutzerrollen zuordnet (Seite 37).
- **Rollenzuordnungsregeln** geben die Bedingungen an, die ein Benutzer erfüllen muss, damit ihn das IVE zu einer oder mehreren Rollen zuweist. Diese Bedingungen beruhen entweder auf den Benutzerinformationen, die der Verzeichnisserver des Bereichs zurückgibt, oder auf dem Benutzernamen des Benutzers (Seite 37).

Authentifizierungsserver

Bei einem ***Authentifizierungsserver*** handelt es sich um eine Datenbank, in der Anmeldeinformationen für Benutzer (Benutzername und Kennwort) und normalerweise Gruppeninformationen gespeichert werden. Wenn sich ein Benutzer am IVE anmeldet, gibt er einen Authentifizierungsbereich an, der einem Authentifizierungsserver zugeordnet ist. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie erfüllt, leitet das IVE die Anmeldeinformationen des Benutzers an den zugeordneten Authentifizierungsserver weiter. Der Authentifizierungsserver überprüft die Existenz und Identität der Benutzer. Anschließend sendet der Authentifizierungsserver die Bestätigung und, wenn der Server in dem Bereich auch Verzeichnis-/Attributserver verwendet wird, auch die Gruppeninformationen des Benutzers oder andere Benutzerattributinformationen an das IVE. Das IVE ermittelt die Rollenzuordnungsregeln für den Bereich und die Benutzerrollen, denen ein Benutzer zugeordnet werden kann.

Zum Angeben eines Authentifizierungsservers, der für einen Bereich verwendet werden kann, müssen Sie zunächst auf der Seite **System > Signing In > Servers** eine Serverinstanz konfigurieren. Wenn Sie die

Servereinstellungen speichern, wird der Servername (der der Instanz zugewiesene Name) auf der Registerkarte **General** des Bereichs in der Dropdownliste **Authentication Server** angezeigt. Wenn es sich beim Server um einen LDAP- oder Active Directory-Server handelt, wird auch der Name der Instanz auf der Registerkarte **General** des Bereichs in der Dropdownliste **Directory/Attribute server** angezeigt. Sie können denselben LDAP- oder Active Directory-Server in einem Bereich für Authentifizierung und Autorisierung verwenden, oder Sie verwenden dieselbe Serverinstanz zur Authentifizierung in einem Bereich und zur Autorisierung in verschiedenen anderen Bereichen, in denen andere Server zur Authentifizierung verwendet werden.

Das NetScreen Instant Virtual Extranet unterstützt die gängigen Authentifizierungsserver, z.B. Windows NT-Domäne, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server und Netegrity SiteMinder. Sie können eine oder mehrere lokale Datenbanken für Benutzer erstellen, die vom IVE authentifiziert wurden. Einen Überblick über Server und Informationen zur Konfiguration finden Sie unter:

- Konfigurieren einer ACE/Serverinstanz 215
- Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz 221
- Konfigurieren einer Instanz eines anonymen Servers 223
- Konfigurieren einer Zertifikatserverinstanz 225
- Konfigurieren einer LDAP-Serverinstanz 229
- Konfigurieren einer lokalen IVE-Server-Instanz 235
- Konfigurieren einer Netegrity SiteMinder-Instanz 247
- Konfigurieren einer NIS-Serverinstanz 241
- Konfigurieren einer RADIUS-Serverinstanz 243

Hinweis: Ein Authentifizierungsserver muss eine Verbindung mit dem IVE-Server herstellen können. Wenn ein Authentifizierungsserver wie RSA ACE/Server keine IP-Adressen für die Agent-Hosts verwendet, muss er den IVE-Hostnamen über einen DNS-Eintrag oder einen Eintrag in der eigenen Hostdatei auflösen können.

Authentifizierungsrichtlinien

Eine ***Authentifizierungsrichtlinie*** besteht aus einer Reihe von Regeln für einen Aspekt der Zugriffsverwaltung, die steuern, ob dem Benutzer eine Anmeldeseite für den Bereich angezeigt wird.
Eine Authentifizierungsrichtlinie ist Bestandteil der Konfiguration eines Authentifizierungsbereichs. Sie gibt die Regeln für das IVE an, die vor dem Anzeigen einer Anmeldeseite berücksichtigt werden müssen. Wenn der Benutzer die Anforderungen der Authentifizierungsrichtlinie für den Bereich erfüllt, zeigt das IVE dem Benutzer die Anmeldeseite an und leitet die

Anmeldeinformationen des Benutzers an den entsprechenden Authentifizierungsserver weiter. Wenn der Benutzer durch den Server authentifiziert wird, beginnt das IVE mit der Rollenauswertung.

Verzeichnisserver

Ein ***Verzeichnisserver*** ist eine Datenbank, in der Benutzer- und meistens Gruppeninformationen gespeichert werden. Sie können einen Authentifizierungsbereich so konfigurieren, dass ein Verzeichnisserver Benutzer- oder Gruppeninformationen abruft, die in Rollenzuordnungsregeln und Ressourcenrichtlinien verwendet werden. Gegenwärtig unterstützt das IVE hierfür LDAP-Server, ein LDAP-Server kann daher zur Authentifizierung und Autorisierung verwendet werden. Sie müssen nur eine Serverinstanz definieren, dann wird der Name der LDAP-Serverinstanz in den Dropdownlisten **Authentication Server** und **Directory/Attribute Server** auf der Registerkarte **General** des Bereichs angezeigt. Sie können denselben Server für eine unbeschränkte Anzahl von Bereichen verwenden.

Neben einem LDAP-Server können Benutzerattribute auch mit einem RADIUS-Server abgerufen werden, um sie in Rollenzuordnungsregeln zu verwenden. Eine RADIUS-Serverinstanz wird jedoch im Gegensatz zu einer LDAP-Serverinstanz nicht in den Dropdownlisten des Bereichs und von **Directory/Attribute Server** angezeigt. Um einen RADIUS-Server zum Abrufen von Benutzerinformationen zu verwenden, müssen Sie nur seine Instanz in der Liste **Authentication Server** angeben und dann in der Liste **Directory/Attribute server** die Option **None** auswählen. Dann konfigurieren Sie Rollenzuordnungsregeln, um Attribute des RADIUS-Servers zu verwenden, die in einer Attributliste auf der Seite **Role Mapping Rule** verfügbar sind, nachdem **Rule based on User attribute** ausgewählt wurde.

Weitere Informationen zum Angeben eines Verzeichnisservers finden Sie unter „Erstellen eines Authentifizierungsbereichs“ auf Seite 273. Weitere Informationen zum Angeben von LDAP- oder RADIUS-Attributen in Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 277.

Rollenzuordnungsregeln

Eine ***Rollenzuordnungsregel*** ist eine Anweisung, die in folgendem Format angegeben wird:

Wenn die angegebene Bedingung wahr|nicht wahr ist, dann ordne den Benutzer den ausgewählten Rollen zu.

Sie erstellen eine Rollenzuordnungsregel auf der Registerkarte **Role Mapping**[1] eines Authentifizierungsbereichs. Wenn Sie auf dieser Registerkarte auf **New Rule** klicken, wird die Seite **Role Mapping Rule** angezeigt. Sie enthält einen integrierten Editor für die Definition von Regeln. Der Editor führt Sie durch die drei Schritte, die zum Erstellen einer Regel notwendig sind:

1. Geben Sie den Bedingungstyp an, auf dem die Regel beruhen soll. Folgende Optionen stehen zur Verfügung:
   - Benutzername
   - Benutzerattribut
   - Zertifikat oder Zertifikatsattribut
   - Gruppenmitgliedschaft
   - Benutzerdefinierte Ausdrücke
2. Geben Sie die auszuwertende Bedingung an, die sich folgendermaßen zusammensetzt:
   1. Angeben von einem oder mehreren Benutzernamen, Benutzerattributen, Zertifikatsattributen, Gruppen (LDAP) oder Ausdrücken, die von dem in Schritt 1 ausgewählten Bedingungstyp abhängen.
   2. Angeben der Wertentsprechungen. Dies kann auch eine Liste von IVE-Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statisch oder im Vergleich mit LDAP-Attributen), LDAP-Gruppen oder vordefinierten Ausdrücken umfassen.
3. Geben Sie die Rollen an, die dem authentifizierten Benutzer zugewiesen werden sollen.

Das IVE stellt eine Liste aller ***zulässigen Rollen*** zusammen, denen ein Benutzer zugeordnet werden kann. Diese Rollen ergeben sich aus den Rollenzuordnungsregeln, denen ein Benutzer entspricht. Anschließend wertet das IVE die Definitionen der einzelnen Rollen aus, um festzustellen, ob der Benutzer Rolleneinschränkungen unterliegt. Auf dem IVE werden diese Informationen verwendet, um eine Liste ***gültiger Rollen*** zu erstellen. Dies sind Rollen, für die der Benutzer zusätzliche Anforderungen erfüllt. Abschließend führt das IVE entweder eine permissive Zusammenführung der gültigen Rollen durch oder zeigt dem Benutzer eine Liste gültiger Rollen an. Dies hängt von der Konfiguration ab, die auf der Registerkarte **Role Mapping** des Bereichs angegeben ist.

1. Administratoren erstellen Rollenzuordnungsregeln auf der Registerkarte Administrators > Authentication > *Ausgewählter Bereich* > Role Mapping. Benutzer erstellen Rollenzuordnungsregeln auf der Registerkarte Users > Authentication > *Ausgewählter Bereich* > Role Mapping.

Weitere Informationen über Rollen finden Sie unter „Benutzerrollen – Übersicht“ auf Seite 55. Weitere Informationen über das Angeben von Rollenzuordnungsregeln finden Sie unter „Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich“ auf Seite 277.

Ressourcenrichtlinien – Übersicht

Eine ***Ressourcenrichtlinie*** ist eine Richtlinie, die Ressourcen und Aktionen für eine bestimmte Zugriffsfunktion angibt. Eine Ressource kann entweder ein Server oder eine Datei sein, auf die über das IVE zugegriffen werden kann. Mithilfe einer Aktion wird einer Ressource „erlaubt" oder „verboten", eine Funktion durchzuführen. Jede Zugriffsfunktion verfügt über mindestens einen Richtlinientyp, der die Antwort des IVE auf eine Benutzeranfrage oder die Art bestimmt, wie eine Zugriffsfunktion aktiviert wird (im Fall von Secure Meeting und E-Mail-Client). Sie können auch detaillierte Regeln für eine Ressourcenrichtlinie definieren, mit denen Sie zusätzliche Anforderungen für bestimmte Benutzeranforderungen auswerten können.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

Typen von Ressourcenrichtlinien 41
Bestandteile einer Ressourcenrichtlinie 42
Auswerten von Ressourcenrichtlinien 43
Angeben von Ressourcen für eine Ressourcenrichtlinie..... 45
Schreiben einer detaillierten Regel 52

Typen von Ressourcenrichtlinien

- **Webressourcenrichtlinien** – Die Webzugriffsfunktion verfügt über die folgenden Typen von Ressourcenrichtlinien:
  - Access: Gibt Webressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 330)
  - Caching: Gibt an, für welche Webressourcen das IVE Seitenheader sendet oder ändert (Seite 331)
  - Java Access: Gibt die Server an, mit denen Java-Applets eine Verbindung herstellen können (Seite 336)
  - Java Signing: Gibt an, ob Java-Applets mit einem Appletzertifikat oder dem Standard-IVE-Zertifikat neu signiert werden (Seite 336)
  - Selective Rewriting: Gibt an, welche Ressourcen das IVE neu schreiben kann (Seite 340)
  - Pass through Proxy: Gibt Webanwendungen an, für die das IVE eine minimale Vermittlung durchführt (Seite 348)
  - Form POST: Gibt an, ob die IVE-Anmeldeinformationen eines Benutzers direkt an ein Anmeldeformular einer Backend-Webanwendung gesendet werden (Seite 342)
  - Cookies/Headers: Gibt an, ob Cookies und Header an ein Anmeldeformular einer Backend-Webanwendung gesendet werden (Seite 342)

- **Dateiressourcenrichtlinien** – Die Dateizugriffsfunktion verfügt über die folgenden Typen von Ressourcenrichtlinien:
  - Windows Access: Gibt Windows-Dateiressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 352)
  - Windows Credentials: Gibt Windows-Dateiressourcen an, für die Sie oder Benutzer zusätzliche Anmeldeinformationen angeben müssen (Seite 352)
  - UNIX/NFS Access: Gibt UNIX/NFS-Dateiressourcen an, zu denen Benutzer navigieren bzw. nicht navigieren dürfen (Seite 358)
- **Secure Application Manager-Ressourcenrichtlinien** – Die Secure Application Manager-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinien: Diese erlaubt oder verweigert Anwendungen, die zum Verwenden von J-SAM oder W-SAM konfiguriert sind, die Herstellung von Socketverbindungen (Seite 361)
- **Telnet/SSH-Ressourcenrichtlinien** – Die Telnet/SSH-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinien: Diese erlaubt oder verweigert den Zugriff auf die angegebenen Server (Seite 365)
- **Network Connect-Ressourcenrichtlinien** – Die Network Connect-Zugriffsfunktion verfügt über zwei Typen von Ressourcenrichtlinien: Diese erlaubt oder verweigert den Zugriff auf die angegebenen Server und gibt IP-Adresspools an (Seite 369)
- **Secure Application Manager-Ressourcenrichtlinien** – Die Secure Application Manager-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinien: Diese aktiviert oder deaktiviert E-Mail-Benachrichtigungen an Benutzer, die zu einer Secure Meeting-Konferenz eingeladen wurden (Seite 375)
- **Secure Email Client-Ressourcenrichtlinien** – Die Secure Email Client-Zugriffsfunktion verfügt über einen Typ von Ressourcenrichtlinien: Diese aktiviert oder deaktiviert E-Mail-Client-Unterstützung (Seite 379)

Bestandteile einer Ressourcenrichtlinie

Eine Ressourcenrichtlinie enthält die folgenden Informationen:

- **Ressourcen:** Eine Reihe von Ressourcennamen (URLs, Hostnamen oder Kombinationen aus IP-Adresse/Netzmaske), die die Ressourcen angeben, für die die Richtlinie gilt. Sie können eine Ressource mit einem Platzhalterpräfix angeben, das für einen Hostnamen steht. Die Standardressource für eine Richtlinie wird durch ein Sternchen (*) angegeben, d.h., die Richtlinie gilt für alle entsprechenden Ressourcen.

Weitere Informationen finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 45.

- **Rollen:** Eine optionale Liste von Benutzerrollen, für die diese Richtlinie gilt. Standardmäßig gilt die Richtlinie für alle Rollen.
- **Aktion:** Die Aktion, die das IVE durchführt, wenn ein Benutzer die Ressource entsprechend der Liste **Ressource** anfordert. Eine Aktion kann angeben, ob der Zugriff auf eine Ressource erlaubt oder verboten ist oder ob eine Aktion durchgeführt wird (z.B. das Neuschreiben von Webinhalt oder das Zulassen von Java-Socketverbindungen).
- **Detaillierte Regeln:** Eine optionale Liste von Elementen, die Ressourcendetails angibt (z.B. bestimmte URLs, Verzeichnispfade, Dateien oder Dateitypen), auf die eine andere Aktion angewendet werden soll oder für die vor der Anwendung der Aktion Bedingungen ausgewertet werden sollen. Sie können eine oder mehrere Regeln definieren und die Reihenfolge angeben, in der das IVE diese auswertet. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

Auswerten von Ressourcenrichtlinien

Wenn das IVE eine Benutzeranforderung erhält, wertet es die dem Anforderungstyp entsprechenden Ressourcenrichtlinien aus. Beim Verarbeiten der Richtlinie, die der angeforderten Ressource entspricht, führt es die angegebene Aktion für die Anforderung aus. Diese Aktion ist auf der Registerkarte **General** oder **Detailed Rules** der Richtlinie festgelegt. Wenn ein Benutzer beispielsweise eine Webseite anfordert, „weiß“ das IVE, wie die Webressourcenrichtlinien zu verwenden sind. Im Fall von Webanforderungen startet das IVE immer mit den Richtlinien für „Web Rewriting“ (Neuschreiben von Webinhalt), „Selective Rewriting“ (selektives Neuschreiben) und „Pass Through Proxy“ (Durchgangsproxy), um zu bestimmen, ob die Anforderung verarbeitet werden soll. Wenn keine dieser Richtlinien angewendet werden kann (oder keine definiert ist), wertet das IVE die Richtlinien für „Web Access“ (Webzugriff) aus, bis es eine findet, die zur angefragten Ressource gehört.

Das IVE wertet eine Gruppe von Ressourcenrichtlinien für eine Zugriffsfunktion von oben nach unten aus, d.h. es startet mit der ersten Richtlinie und durchläuft dann die Liste, bis eine passende Richtlinie gefunden wird. Wenn Sie detaillierte Regeln für die passende Richtlinie definiert haben, wertet das IVE die Regeln von oben nach unten aus und stoppt, wenn es in der Liste **Resource** der Regel eine passende Ressource findet. In der folgenden Abbildung werden die allgemeinen Schritte der Richtlinienauswertung dargestellt:

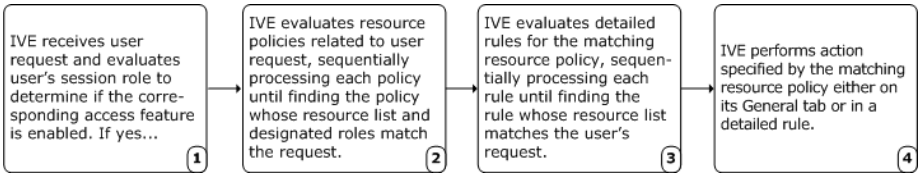

IVE receives user request and evaluates user's session role to determine if the corresponding access feature is enabled. If yes...
1
IVE evaluates resource policies related to user request, sequentially processing each policy until finding the policy whose resource list and designated roles match the request.
2
IVE evaluates detailed rules for the matching resource policy, sequentially processing each rule until finding the rule whose resource list matches the user's request.
3
IVE performs action specified by the matching resource policy either on its General tab or in a detailed rule.
4

Abbildung 3:Schritte bei der Auswertung von Ressourcenrichtlinien

Details der einzelnen Auswertungsschritte:

1. Die „Sitzungsrolle" eines Benutzers basiert auf der Rolle bzw. den Rollen, der bzw. denen er während des Authentifizierungsvorgangs zugewiesen wird. Die für einen Benutzer aktivierten Zugriffsfunktionen werden durch eine Rollenzuordnungskonfiguration des Authentifizierungsbereichs bestimmt.
2. Die Funktionen für Web- und Dateizugriff verfügen über mehrere Typen von Ressourcenrichtlinien. Das IVE ermittelt daher zunächst den Anforderungstyp (z.B. auf eine Webseite, ein Java-Applet oder eine UNIX-Datei) und wertet dann die der Anforderung entsprechenden Ressourcenrichtlinien aus. Für die Webzugriffsfunktion werden z.B. für jede Webanforderung zuerst die Richtlinien zum Neuschreiben ausgewertet. Die verbleibenden fünf Zugriffsfunktionen, Secure Application Manager, Secure Terminal Access, Secure Meeting und Secure Email Client, verfügen über nur eine Ressourcenrichtlinie.
3. Mit einer detaillierten Regel können die folgenden beiden Vorgänge durchgeführt werden:
   - Ressourcen, für die eine Aktion gilt, können auf einer genaueren Ebene angegeben werden. Wenn Sie z.B. in den Hauptrichtlinien-Einstellungen einer Webzugriffs-Ressourcenrichtlinie einen Webserver angeben, können Sie eine detaillierte Regel definieren, die einen bestimmte Pfad auf diesem Server angibt, und dann die Aktion für diesen Pfad ändern.
   - Es kann vom Benutzer verlangt werden, dass er zum Anwenden der Aktion bestimmte Bedingungen erfüllt, die in Form boolescher Ausdrücke oder benutzerdefinierter Ausdrücke geschrieben wurden. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52).
4. Das IVE beendet die Verarbeitung von Ressourcenrichtlinien, sobald die angeforderte Ressource in der Liste **Resource** einer Richtlinie oder in einer detaillierten Regel gefunden wird.

Angeben von Ressourcen für eine Ressourcenrichtlinie

Für das IVE-Modul, dass Ressourcenrichtlinien auswertet, müssen die in der Liste **Resources** einer Richtlinie aufgelisteten Ressourcen im kanonischen Format aufgeführt sein. In diesem Abschnitt werden die kanonischen Formate beschrieben, die zum Angeben von Web-, Datei- und Serverressourcen verfügbar sind. Wenn ein Benutzer versucht, auf eine bestimmte Ressource zuzugreifen, vergleicht das IVE die angeforderte Ressource mit der in den entsprechenden Richtlinien angegebenen Ressource. Es beginnt dabei mit der ersten Richtlinie in der Richtlinienliste. Wenn das Modul eine angeforderte Ressource mit einer in der Liste **Resources** einer Richtlinie angegebenen Ressource abgleicht, wertet es weitere Richtlinieneinschränkungen aus und gibt die entsprechende Aktion an das IVE zurück. (Es werden keine weiteren Richtlinien ausgewertet.) Wenn keine Richtlinie zutrifft, wertet das IVE Lesezeichen für automatische Erlaubnis (sofern definiert) aus, andernfalls wird die Standardaktion für die Richtlinie zurückgegeben.

Die erforderlichen kanonischen Formate werden in folgenden Abschnitten beschrieben:

- Angeben von Webressourcen (46)
- Angeben von Windows-Dateiressourcen (48)
- Angeben von UNIX/NFS-Dateiressourcen (49)
- Angeben von Serverressourcen (50)
- Angeben von IP-Adresspools (51)

Allgemeine Anmerkungen zu kanonischen Formaten

- Wenn eine Pfadkomponente mit einem Schrägstrich und einem Sternchen endet (/*), entspricht dies dem untergeordneten Knoten und allen weiteren Unterverzeichnissen. Wenn eine Pfadkomponente mit einem Schrägstrich und einem Prozentzeichen endet (/%), entspricht dies dem untergeordneten Knoten und allen Elementen, die sich genau einer Ebene darunter befinden.

  Beispiel:

  /intranet/* entspricht Folgendem:

  /intranet

  /intranet/home.html

  /intranet/elee/public/index.html

  /intranet/% entspricht Folgendem:

/intranet

/intranet/home.html

but NOT /intranet/elee/public/index.html

- Der Hostname und die IP-Adresse einer Ressource werden gleichzeitig an das Richtlinienmodul weitergegeben. Wenn ein Server in der Liste **Resources** einer Richtlinie als IP-Adresse angegeben ist, erfolgt die Auswertung anhand der IP-Adresse. Andernfalls versucht das Modul, die beiden Hostnamen abzugleichen. Es führt kein Reverse-DNS-Lookup zur Ermittlung der IP-Adresse durch.
- Wenn ein Hostname in der Liste **Resources** einer Richtlinie nicht vollständig qualifiziert ist, wenn z.B. „netscreen" anstelle von „intranet.netscreen.net" angegeben ist, führt das Modul die Auswertung anhand der vorliegenden Angaben durch, der Hostname wird nicht weiter qualifiziert.

Angeben von Webressourcen

Kanonisches Format: `[Protokoll://]Host[:Ports][/Pfad]`

Die vier Bestandteile sind:

- **Protokoll** (optional)

  Mögliche Werte: `http` und `https` (Groß- oder Kleinschreibung wird nicht berücksichtigt)

  Wenn das Protokoll fehlt, werden sowohl `http` als auch `https` angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „`://`" eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host** (erforderlich)

  Mögliche Werte:

  - **DNS-Hostname**

    Beispiel: www.netscreen.com

    Sonderzeichen sind zulässig, einschließlich:

    ***** Entspricht ALLEN Zeichen

    % Entspricht einem beliebigen Zeichen außer dem Punkt (.)

    ? Entspricht genau einem Zeichen

- **IP-Adresse/Netzmaske**
  Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`
  Die Netzmaske kann eins der beiden Formate aufweisen:
  - Präfix: Obere Bits
  - IP: `a.b.c.d`

  Beispiel: `10.11.149.2/24` oder `10.11.149.2/255.255.255.0`
  Sonderzeichen sind nicht zulässig.

- **Ports** (optional)
  Mögliche Werte:

*****	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommas getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

Hinweis: Sie können Portlisten und Portbereiche mischen.
Beispiel: 80,443,8080-8090

Wenn kein Port angegeben ist, wird der Standardport 80 für `http` und 443 für `https` zugewiesen. Bei der Angabe eines Ports muss das Trennzeichen „:" eingegeben werden.

- **Pfad** (optional)
  Wenn kein Pfad angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Bei der Angabe eines Pfades muss das Trennzeichen „/" eingegeben werden. Es werden keine weiteren Sonderzeichen unterstützt.

  Beispiele:
  - http://www.netscreen.com:80/*
  - https://www.netscreen.com:443/intranet/*
  - *.yahoo.com:80,443/*
  - %.danastreet.net:80/share/users/<USER>/*

Angeben von Windows-Dateiressourcen

Kanonisches Format: `\\Server[\Freigabe[\Pfad]]`

Die drei Bestandteile sind:

- **Server** (erforderlich)

  Mögliche Werte:

  - **Hostname**

    Die Systemvariable <USER> kann verwendet werden.

  - **IP-Adresse**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.

- **Freigabe** (optional)

  Wenn keine Freigabe angegeben ist, wird von einem Sternchen (*) ausgegangen, was bedeutet, dass ALLE Pfade zutreffen. Die Systemvariable <USER> darf verwendet werden.

- **Pfad** (optional)

  Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer einem umgekehrten Schrägstrich (\)
?	Entspricht genau einem Zeichen

  Wenn kein Pfad angegeben ist, wird von einem umgekehrten Schrägstrich (\) ausgegangen, d.h. es werden nur die Ordner der obersten Ebene berücksichtigt.

  Beispiele:

  - \\%.danastreet.net\share\<USER>*
  - *.netscreen.com\dana*
  - \\10.11.0.10\share\web*
  - \\10.11.254.227\public\%.doc

Angeben von UNIX/NFS-Dateiressourcen

Kanonisches Format: `Server[/Pfad]`

Die beiden Bestandteile sind:

- **Server** (erforderlich)

  Mögliche Werte:

  - **Hostname**

    Die Systemvariable <USER> kann verwendet werden.

  - **IP-Adresse**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

  Die beiden vorangehenden umgekehrten Schrägstriche (\\) sind erforderlich.

- **Pfad** (optional)

  Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht einem beliebigen Zeichen
%	Entspricht einem beliebigen Zeichen außer einem umgekehrten Schrägstrich (\)
?	Entspricht genau einem Zeichen

  Wenn kein Pfad angegeben ist, wird von einem umgekehrten Schrägstrich (\) ausgegangen, d.h. es werden nur die Ordner der obersten Ebene berücksichtigt.

  Beispiele:

  - %.danastreet.net/share/users/<USER>/*
  - *.netscreen.com/dana/*
  - 10.11.0.10/web/*
  - 10.11.254.227/public/%.txt

Angeben von Serverressourcen

Kanonisches Format: `[Protokoll://]Host[:Ports]`

Die drei Bestandteile sind:

- **Protokoll** (optional)

  Hinweis: Nur für Network Connect-Richtlinien verfügbar. Für weitere Ressourcenrichtlinien für Zugriffsfunktionen wie Secure Application Manager oder Telnet/SSH ist die Angabe dieser Bestandteile ungültig.

  Mögliche Werte (Groß- oder Kleinschreibung wird nicht berücksichtigt):

  - tcp
  - udp
  - icmp

  Wenn kein Protokoll angegeben ist, werden alle drei Protokolle angenommen. Bei der Eingabe eines Protokolls muss das Trennzeichen „://" eingegeben werden. Sonderzeichen sind nicht zulässig.

- **Host** (erforderlich)

  Mögliche Werte:

  - **DNS-Hostname**

    Beispiel: www.netscreen.com

    Sonderzeichen sind zulässig, einschließlich:

*****	Entspricht ALLEN Zeichen
%	Entspricht einem beliebigen Zeichen außer dem Punkt (.)
?	Entspricht genau einem Zeichen

  - **IP-Adresse/Netzmaske**

    Die IP-Adresse muss das folgende Format aufweisen: `a.b.c.d`

    Die Netzmaske kann eins der beiden Formate aufweisen:

    - Präfix: Obere Bits
    - IP: `a.b.c.d`

    Beispiel: `10.11.149.2/24` oder `10.11.149.2/255.255.255.0`

    Sonderzeichen sind nicht zulässig.

- **Ports** (optional)

  Mögliche Werte:

*****	Entspricht ALLEN Ports, andere Sonderzeichen sind nicht zulässig.
Port[,Port]*	Eine durch Kommas getrennte Liste einzelner Ports. Gültige Portnummern sind [1-65535].
[Port 1]-[Port 2]	Ein Portbereich, von Port 1 bis Port 2 einschließlich.

  Hinweis: Sie können Portlisten und Portbereiche mischen.
  Beispiel: 80,443,8080-8090

  Wenn kein Port angegeben ist, wird der Standardport 80 für `http` und 443 für `https` zugewiesen. Bei der Angabe eines Ports muss das Trennzeichen „:" eingegeben werden.

  Beispiele:

  - <USER>.danastreet.net:5901-5910
  - 10.10.149.149:22,23
  - tcp://10.11.0.10:80
  - udp://10.11.0.10:*

Angeben von IP-Adresspools

Kanonisches Format: `IP_Bereich`

Der IP-Bereich kann im Format „`a.b.c.d-e`" angegeben werden, wobei der letzte Bestandteil der IP-Adresse ein durch einen Bindestrich (-) begrenzter Bereich ist. Sonderzeichen sind nicht zulässig.

Beispiel:

10.10.10.1-100

Schreiben einer detaillierten Regel

Mit den Zugriffsfunktionen für Web, Dateien, Secure Application Manager, Telnet/SSH und Network Connect können Sie Ressourcenrichtlinien für einzelne Web-, Datei-, Anwendungs- und Telnet-Server angeben. Die Zugriffsfunktionen für Secure Meeting und Email Client verfügen jeweils über eine global anwendbare Richtlinie. Für diese beiden Richtlinien geben Sie Servereinstellungen an, die für alle Rollen verwendet werden, durch die diese Zugriffsfunktionen ermöglicht werden. Für alle anderen Zugriffsfunktionen können Sie eine beliebige Anzahl von Ressourcenrichtlinien angeben und für jede eine oder mehrere detaillierte Regeln definieren.

Eine ***detaillierte Regel*** ist eine Erweiterung einer Ressourcenrichtlinie, die Folgendes angeben kann:

- Zusätzliche[1] Ressourceninformationen (wie bestimmte Pfade, Dateien oder Dateitypen) für Ressourcen, die auf der Registerkarte **General** aufgelistet sind.
- Eine Aktion, die von der auf der Registerkarte **General** angegebenen Aktion abweicht (obwohl die Optionen die gleichen sind).
- Bedingungen, die erfüllt sein müssen, damit die detaillierte Regel angewendet werden kann.

In vielen Fällen ermöglicht die Basis-Ressourcenrichtlinie, d.h. die auf der Registerkarte **General** einer Ressourcenrichtlinie angegebenen Informationen, ausreichende Zugriffssteuerung für eine Ressource:

> Wenn ein Benutzer, der (definierte_Rollen) angehört, versucht, auf (definierte_Ressourcen) zuzugreifen, FÜHRE die angegebene (Ressourcen_Aktion) aus.

Sie können eine oder mehrere detaillierte Rollen für eine Richtlinie definieren, wenn Sie eine Aktion durchführen möchten, die auf einer Kombination anderer Informationen basiert, zu denen Folgende gehören können:

1. Beachten Sie, dass Sie die gleiche Ressourcenliste (wie auf der Registerkarte **General**) auch als detaillierte Regel angeben können, wenn deren einziger Zweck die Anwendung von Bedingungen auf eine Benutzeranforderung ist.

- Die Eigenschaften einer Ressource, beispielsweise Header, Inhaltstyp oder Dateityp
- Die Eigenschaften eines Benutzers, beispielsweise der Benutzername und die Rollen, denen er zugeordnet ist
- Die Eigenschaften einer Sitzung, beispielsweise die Quell-IP oder der Browsertyp eines Benutzers, ob der Benutzer die Hostprüfung oder Cachebereinigung ausführt, die Uhrzeit oder Zertifikatattribute

Mit detaillierten Regeln kann die Ressourcenzugriffssteuerung flexibler gestaltet werden, das bestehende Ressourcen- oder Berechtigungsinformationen zum Angeben anderer Anforderungen für andere Benutzer verwendet können, auf die die Basisressourcenrichtlinie angewendet wird.

So schreiben Sie eine detaillierte Regel für eine Ressourcenrichtlinie:

1. Geben Sie auf der Seite **New Policy** für eine Ressourcenrichtlinie die erforderlichen Ressourcen- und Rolleninformationen ein.
2. Wählen Sie im Bereich **Action** die Option **Use Detailed Rules** aus, und klicken Sie auf **Save Changes**.
3. Klicken Sie auf der Registerkarte **Detailed Rules** auf **New Rule**.
4. Führen Sie auf der Seite **Detailed Rule** Folgendes aus:
   1. Konfigurieren Sie im Bereich **Action** die Aktion, die ausgeführt werden soll, wenn die Benutzeranforderung einer Ressource in der Liste **Resource** entspricht (optional). Beachten Sie, dass die auf der Registerkarte **General** angegebene Aktion standardmäßig übertragen wird.
   2. Geben Sie im Bereich **Resources** eine der folgenden Optionen an (erforderlich):
      - Die vollständige oder einen Teil der Ressourcenliste, die auf der Registerkarte **General** angegeben ist.
      - Einen bestimmten Pfad oder eine bestimmte Datei auf den Servern, die auf der Registerkarte **General** angegeben sind. Gegebenenfalls können Platzhalter verwendet werden. Informationen zum Verwenden von Platzhaltern in einer **Resources**-Liste finden Sie in der Dokumentation der entsprechenden Ressourcenrichtlinie.
      - Ein Dateityp, dem gegebenenfalls ein Pfad vorangestellt ist, oder geben Sie einfach `*/*.`*`Dateierweiterung`* an, um Dateien mit der angegebenen Erweiterung innerhalb aller Pfade auf den Servern anzuzeigen, die auf der Registerkarte **General** angegeben sind.

3 Geben Sie im Abschnitt **Conditions** mindestens einen Ausdruck an, der für die Ausführung der Aktion ausgewertet wird (optional):

- Boolesche Ausdrücke: Schreiben Sie unter Verwendung von Systemvariablen mindestens einen boolschen Ausdruck mit den Operatoren NOT, OR oder AND. Eine Liste der in Ressourcenrichtlinien verfügbaren Variablen finden Sie unter „Systemvariablen und Beispiele“ auf Seite 442.
- Benutzerdefinierte Ausdrücke: Schreiben Sie unter Einhaltung der entsprechenden Syntax mindestens einen benutzerdefinierten Ausdruck. Informationen zur Syntax und zu Variablen finden Sie unter „Schreiben benutzerdefinierter Ausdrücke“ auf Seite 437. Beachten Sie, dass benutzerdefinierte Ausdrücke nur mit der erweiterten Lizenz verfügbar sind.

4 Klicken Sie auf **Save Changes**.

5. Ordnen Sie die Regeln auf der Registerkarte **Detailed Rules** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Sobald das IVE für die vom Benutzer angeforderte Ressource eine entsprechende Ressource in der Liste **Resource** für eine Regel findet, wird die angegebene Aktion durchgeführt und die Verarbeitung der Regeln (und weiterer Ressourcenrichtlinien) beendet.

Benutzerrollen – Übersicht

Eine ***Benutzerrolle*** ist eine Einheit, die die folgenden Einstellungen festlegt: Parameter für Benutzersitzungen (Sitzungseinstellungen und -optionen), individuelle Einstellungen (benutzerdefinierte Einrichtung der Oberfläche und Lesezeichen) und aktivierte Zugriffsfunktionen (Web-, Datei-, Anwendungs-, Netzwerk-, Konferenz- und E-Mail-Zugriff). Eine Benutzerrolle steuert werden den Ressourcenzugriff noch gibt sie andere ressourcenbasierte Optionen für einzelne Anforderungen an. Mithilfe einer Benutzerrolle kann z. B. definiert werden, ob ein Benutzer über die Berechtigung zum Webbrowsing verfügt. Die einzelnen Webressourcen, auf die ein Benutzer zugreifen darf, werden jedoch durch Webressourcenrichtlinien definiert, die separat konfiguriert werden.

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

Rollenarten 55
Rollenkomponenten 56
Rollenauswertung 58

Informationen zum Erstellen einer Benutzerrolle finden Sie unter „Konfigurieren der Seite „Roles"" auf Seite 285.

Rollenarten

Das IVE unterstützt zwei Arten von Benutzerrollen:

- **Administratoren**

  Eine Administratorrolle ist eine Einheit, die die IVE-Verwaltungsfunktionen und -Sitzungseigenschaften für Administratoren angibt, die der Rolle zugeordnet sind. Sie können eine Administratorrolle anpassen, indem Sie Gruppen von IVE-Funktionen und Benutzerrollen auswählen, die Mitglieder der Administratorrolle anzeigen und verwalten dürfen. Weitere Informationen finden Sie unter „Delegierte Administration – Übersicht" auf Seite 83.

- **Benutzer**

  Eine Benutzerrolle ist eine Einheit, die Parameter für Benutzersitzungen, individuelle Einstellungen und aktivierte Zugriffsfunktionen definiert. Sie können eine Benutzerrolle anpassen, indem Sie bestimmte IVE-Zugriffsfunktion aktivieren, Web-, Anwendungs- und Sitzungs-Lesezeichen definieren und Sitzungseinstellungen für die aktivierten Zugriffsfunktionen konfigurieren. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Roles"" auf Seite 285.

Rollenkomponenten

Eine Benutzerrolle enthält die folgenden Informationen:

- **Rolleneinschränkungen** – Die Verfügbarkeit der Rolle für die Benutzer beruht auf den Anforderungen bezüglich Quell-IP, clientseitigem Zertifikat, Hostprüfung und Cachebereinigung, die erfüllt sein müssen, damit ein Benutzer einer Rolle zugewiesen wird.
- **Sitzungsparameter** – Sitzungseinstellungen, u.a. für Höchstdauerwerte (Leerlauf, Maximum, Erinnerung), Warnungen bei Zeitüberschreitung, Roamingsitzungen und Einzelanmeldung sowie Sitzungsoptionen, beispielsweise für permanente Kennwortzwischenspeicherung, beständige Sitzungscookies und Verfolgung der Browseranforderungen.
- **Optionen für die Benutzeroberfläche** – Individuelle Einstellungen, einschließlich Anmeldeseite, Kopf- und Fußzeile der Seiten sowie Anzeige der Browsing-Symbolleiste. Wenn der Benutzer mehreren Rollen zugeordnet ist, zeigt das IVE die Benutzeroberfläche entsprechend der ersten Rolle an, der der Benutzer zugeordnet wurde.
- **Webeinstellungen** – Aktivierung/Deaktivierung der Webzugriffsfunktion, Definition der Weblesezeichen für die Rolle und Optionen für das Webbrowsing. Letzteres kann Folgendes umfassen:
  - Browsingoptionen: User can type URLs, Allow Java applets, Mask hostnames while browsing, Unrewritten pages open in new window
  - Lesezeichenoptionen: User can add bookmarks, Auto-allow role bookmarks
  - Cookieoptionen: Persistent cookies
- **Dateieinstellungen** – Aktivierung/Deaktivierung der Dateizugriffsfunktion, Definition der Dateilesezeichen und Optionen für die Dateinavigation. Letzteres kann Folgendes umfassen:
  - Windows-Netzwerkdateien: User can browse network file shares, User can add bookmarks, Users can add personal bookmarks to Windows folders
  - UNIX-Netzwerkdateien: User can browse network file shares, User can add bookmarks, Users can add personal bookmarks to UNIX/NFS directories

- **Telnet/SSH-Einstellungen** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Terminal Access, Lesezeichen für Telnet/SSH-Sitzungseinstellungen für diese Rolle und Telnet/SSH-Optionen. Letzteres kann Folgendes umfassen:
  - User can add sessions
  - Auto-allow role Telnet/SSH sessions
- **SAM-Einstellungen** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Application Manager (J-SAM/W-SAM), Lesezeichen für W-SAM- oder J-SAM-Anwendungen. Letzteres kann Folgendes umfassen:
  - Allgemeine Optionen für Secure Application Manager: Auto-launch Secure Application Manager, Auto-uninstall Secure Application Manager, Auto-allow application servers
  - Optionen für Windows SAM: Auto-upgrade Secure Application Manager
  - Optionen für Java SAM: User can add applications, Automatic host-mapping
- **Einstellungen für Network Connect** – Aktivierung/Deaktivierung der Zugriffsfunktion Network Connect sowie Gewähren von Zugriff auf das lokale Subnetz.
- **Einstellungen für Secure Meeting** – Aktivierung/Deaktivierung der Zugriffsfunktion Secure Meeting und Optionen für Secure Meeting. Dies kann Folgendes umfassen:
  - Allgemeine Optionen: Join and create, authentication requirements, password distribution, remote control
  - Policy settings for number of scheduled meetings, simultaneous meetings, simultaneous meeting attendees, duration of meetings

Konfigurationsanweisungen finden Sie unter „Konfigurieren der Seite „Roles““ auf Seite 285.

Rollenauswertung

Das IVE-Rollenzuordnungsmodul legt die ***Sitzungsrolle*** eines Benutzers fest oder kombinierte Berechtigungen, die gültig für eine Benutzersitzung sind. Dies geschieht folgendermaßen:

1. Das IVE beginnt die Rollenauswertung mit der ersten Regel auf der Registerkarte **Role Mapping**[1] des Authentifizierungsbereichs, an dem sich der Benutzer erfolgreich anmeldet.
2. Das IVE ermittelt, ob der Benutzer die Bedingungen der Regel erfüllt. Wenn dies der Fall ist, führt das IVE Folgendes durch:
   1. Das IVE fügt die entsprechenden Rollen einer Liste von „zulässigen Rollen" hinzu, zu denen der Benutzer zugeordnet werden kann.
   2. Das IVE berücksichtigt dabei, ob konfiguriert wurde, dass die Verarbeitung bei einem Treffer beendet werden soll (Option „Stop on Match"). Wenn dies der Fall ist, fährt das Modul mit Schritt 5 fort.
3. Gemäß Prozessschritt 2 wertet das IVE die nächste Regel aus, die auf der Registerkarte **Role Mapping** des Authentifizierungsbereichs angegeben ist. Dies wird für alle folgenden Regeln wiederholt, bis alle Rollenzuordnungsregeln ausgewertet sind und das IVE eine vollständige Liste der zulässigen Rollen aufgestellt hat.
4. Das IVE wertet die Definitionen aller Rollen in der Liste der zulässigen Rollen aus und überprüft, ob der Benutzer Rolleneinschränkungen unterliegt. Das IVE erstellt anhand dieser Informationen eine Liste der ***gültigen Rollen*** zu erstellen, d.h. der Rollen, für die der Benutzer zusätzliche Anforderungen erfüllt.

   Wenn die Liste gültiger Rollen nur eine Rolle enthält, ordnet das IVE den Benutzer dieser Rolle zu. Andernfalls setzt das IVE die Auswertung fort.
5. Für Benutzer, die mehreren Rollen zugeordnet sind, wertet das IVE die Einstellung aus, die auf der Registerkarte **Role Mapping** angegeben ist.
   - **Merge settings for all assigned roles**

     Wenn Sie diese Option auswählen, führt das IVE eine permissive Zusammenführung aller gültigen Benutzerrollen durch, um die Gesamtrolle (Netzrolle) für eine Benutzersitzung zu ermitteln.
   - **User must select from among assigned roles**

     Wenn Sie diese Option auswählen, gibt das IVE einem authentifizierten Benutzer eine Liste zulässiger Rollen aus. Der Benutzer muss eine Rolle aus der Liste auswählen, und das IVE weist den Benutzer dann für die Dauer der Benutzersitzung dieser Rolle zu.

1. Siehe „Rollenzuordnungsregeln" auf Seite 53.

Richtlinien für permissive Zusammenführungen

Eine ***permissive Zusammenführung*** ist eine Zusammenführung, die *aktivierte* Funktionen und Einstellungen anhand der folgenden Richtlinien kombiniert.

- Die Aktivierung einer Zugriffsfunktion in einer Rolle hat Vorrang vor der Deaktivierung der gleichen Funktion in einer anderen Rolle. Wenn beispielsweise Secure Meeting für eine Rolle, der ein Benutzer angehört, deaktiviert, für eine andere Rolle jedoch aktiviert ist, darf der Benutzer Secure Meeting in dieser Benutzersitzung verwenden.
- Bei Secure Application Manager aktiviert das IVE die Version, die der ersten Rolle entspricht, für die diese Funktion aktiviert ist. Außerdem führt das IVE die Einstellungen aller Rollen zusammen, die der ausgewählten Version entsprechen.
- Bei den Optionen für die Benutzeroberfläche wendet das IVE die Einstellungen an, die der ersten Rolle entsprechen, der der Benutzer zugeordnet ist.
- Bei Überschreitungen der Sitzungsdauer wendet das IVE den höchsten Wert aller Rollen auf die Benutzersitzung an.
- Wenn die Roaming-Sitzungsfunktion für mehrere Rollen aktiviert ist, führt das IVE die Netzmasken zusammen, um die Netzmaske für die Sitzung zu erweitern.

Teil 2
IVE-Funktionen

In diesem Abschnitt werden die Funktionen des Access Series-Produkts beschrieben. Für einige dieser Funktionen sind weitere Lizenzen erforderlich.

Inhalt

Cachebereinigung – Übersicht 63
Central Manager – Übersicht 67
Zertifikate – Übersicht 69
Cluster – Übersicht 75
Delegierte Administration – Übersicht 83
E-Mail-Client – Übersicht 85
Hostprüfung – Übersicht 91
Protokollierung und Überwachung – Übersicht 95
Network Connect – Übersicht 99
Durchgangsproxy – Übersicht 103
Remote SSO – Übersicht 107
Secure Application Manager – Übersicht 109

Cachebereinigung – Übersicht

Bei der Cachebereinigung handelt es sich um einen Client-Agent, der übrig gebliebene Daten wie temporäre Dateien oder Anwendungscaches nach einer IVE-Sitzung vom Benutzercomputer entfernt. Wenn sich beispielsweise ein Benutzer von einem Internet-Kiosk beim IVE anmeldet und mithilfe eines Browser-Plugins ein Microsoft Word-Dokument öffnet, entfernt die Cachebereinigung nach Beenden der Sitzung die im Browsercache (im Ordner „Windows") gespeicherte temporäre Kopie der Word-Datei. Durch das Entfernen der Kopie verhindert die Cachebereinigung, dass andere Benutzer des Kiosks das Word-Dokument suchen und öffnen können, nachdem der IVE-Benutzer seine Sitzung beendet hat.

Sie können den Zugriff auf das IVE und die Ressourcen durch die Cachebereinigung einschränken:

- **Richtlinie für Bereichsauthentifizierung**

  Wenn Administratoren versuchen, sich beim IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus und ermittelt, ob die Cachebereinigung zu den Anforderungen gehört, die vor der Authentifizierung erfüllt sein müssen. Sie können eine Richtlinie für die Bereichsauthentifizierung so konfigurieren, dass die Cachebereinigung heruntergeladen wird, die Cachebereinigung heruntergeladen und ausgeführt wird oder dass die Cachebereinigung nicht erforderlich ist. Der Benutzer muss sich von einem Computer anmelden, der den Cachebereinigung-Anforderungen entspricht, die für den Bereich festgelegt wurden. Wenn dies nicht der Fall ist, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und der Benutzer kann nicht auf das IVE zugreifen.

- **Benutzerrolle**

  Wenn das IVE die Liste der geeigneten Rollen ermittelt, denen ein Administrator oder Benutzer zugeordnet ist, wertet es die Einschränkungen der einzelnen Rollen aus, um zu ermitteln, ob die Rolle die Ausführung der Cachebereinigung auf der Arbeitsstation des Benutzers erfordert. Wenn dies der Fall ist und das Gerät des Benutzers die Cachebereinigung noch nicht ausführt, ordnet das IVE den Benutzer dieser Rolle nicht zu.

- **Ressourcenrichtlinie**

  Wenn ein Benutzer eine Ressource anfordert, wertet das IVE die detaillierten Regeln der Ressourcenrichtlinie aus, um zu ermitteln, ob die Cachebereinigung auf der Arbeitsstation des Benutzers installiert werden muss oder bereits ausgeführt wird. Das IVE verweigert den Zugriff auf die betreffende Ressource, wenn das Gerät des Benutzers nicht der festgelegten Cachebereinigung-Richtlinie entspricht.

Ausführen der Cachebereinigung

Wenn Sie die Cachebereinigung als Anforderung für eine Rolle oder Ressourcenrichtlinie festlegen möchten, muss der Agent bei der Anmeldung des Benutzers minimal installiert werden. Dies wird in der Authentifizierungsrichtlinie des Bereichs konfiguriert. Nach der Konfiguration lädt das IVE das ActiveX-Steuerelement auf das System des Benutzers herunter. Die Cachebereinigung wird in dem Intervall ausgeführt, dass Sie auf der Registerkarte **System > Configuration > Security > Cache Cleaner** konfigurieren[1]. Für die Ausführung der Cachebereinigung muss auf den Benutzercomputern ActiveX aktiviert sein.

Hinweis: ActiveX-Steuerelemente werden für Administratoren und Hauptbenutzer in Windows 2000-Systemen automatisch aktiviert, Standardbenutzer müssen sie hingegen manuell aktivieren. Um ActiveX-Steuerelemente in Internet Explorer zu aktivieren, wählen Sie **Extras > Internetoptionen > Sicherheit > Anpassen** aus, und aktivieren Sie anschließend im Dialogfeld **Sicherheitseinstellungen** die ActiveX-Komponenten.

Cachebereinigung führt in folgenden Situationen eine endgültige Bereinigung aus:

- **Der Benutzer meldet sich explizit von seiner Benutzersitzung ab**

  Wenn ein Benutzer auf der IVE-Startseite auf **Sign Out** klickt, führt die Cachebereinigung eine endgültige Bereinigung aus und deinstalliert sich anschließend selbst vom Benutzersystem.

- **Die Höchstdauer für die Benutzersitzung ist überschritten**

  Wenn eine Zeitüberschreitung auftritt, führt die Cachebereinigung eine Bereinigung durch. Wenn sich der Benutzer erneut anmeldet, führt die Cachebereinigung eine erneute Bereinigung durch. Die Cachebereinigung überprüft in bestimmten Abständen die Gültigkeit einer Sitzung und erkennt, wann eine Zeitüberschreitung auftritt. Die Abstände werden auf der Registerkarte **System > Configuration > Security > Cache Cleaner** angegeben (siehe „Registerkarte „Security > Cache Cleaner"" auf Seite 146).

  Hinweis: Bei der Überprüfung der Gültigkeit einer Sitzung stellt die Cachebereinigung eine Verbindung mit dem IVE her. Durch diese Aktion können an persönlichen Firewalls Warnmeldungen ausgegeben werden. Benutzer müssen diesen Datenverkehr zulassen, damit die Cachebereinigung ordnungsgemäß ausgeführt werden kann.

  ---

1. Benutzern mit einer persönlichen Firewall wird beim Leeren des Cache durch die Cachebereinigung ein Protokolleintrag angezeigt.

- **Ein Clientsystem wird nach einem nicht ordnungsgemäßen Herunterfahren des Systems bzw. einem nicht ordnungsgemäßen Abbruch der Sitzung oder der Verbindung neu gestartet.**

  Die Cachebereinigung führt eine endgültige Bereinigung aus und deinstalliert sich nach dem Neustart des Systems selbst vom Benutzersystem.

Die Cachebereinigung protokolliert keine Einträge im IVE-Standardprotokoll, sondern in einer temporären Client-Textdatei.

```
C:\Programme\Neoteris\Cache Cleaner\dsCacheCleaner.log
```

Dieses Protokoll wird gelöscht, wenn sich die Cachebereinigung selbst deinstalliert.

Wichtig: Die Cachebereinigung bereinigt bzw. löscht weder den Browserverlauf noch vom Benutzer explizit gespeicherten Dateien, Internet Explorer-Plugins, ActiveX-Steuerelemente oder Einträge in `index.dat` (eine private Tabelle von URLs, die vom Internet Explorer verwaltet wird).

Weitere Informationen zu den Optionen der Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 23.

Central Manager – Übersicht

Central Manager ist ein zweischichtiges System (Client/Server) für die Verwaltung mehrerer IVEs, unabhängig davon, ob diese sich in einem Cluster befinden. Central Manager enthält Folgendes:

- **System-Dashboard**

  Die Dashboard-Funktion von Central Manager zeigt Diagramme und Warnhinweise zur Systemkapazität an und ermöglicht Ihnen damit die komfortable Überwachung des Systems. (Seite 125)

- **Verbesserte Protokollierung und Überwachung**

  Sie können eigene Filter für die Protokollierung erstellen, sodass Sie nur ausgewählte Protokollmeldungen im gewünschten Format anzeigen und speichern können. (Seite 187)

- **Konfigurationsübertragung**

  Die Funktion für die Konfigurationsübertragung ermöglicht eine komfortable, zentrale Verwaltung, da Sie Einstellungen ganz einfach von einem IVE auf ein anderes übertragen können. (Seite 399)

- **Ausfallfreie Aktualisierung**

  Die Funktion für ausfallfreie Aktualisierung beschleunigt die Aktualisierung innerhalb eines Clusters, da sie gewährleistet, dass ein Clustermitglied während des Vorgangs immer funktionstüchtig ist. (Seite 384)

- **Verbesserte Benutzeroberfläche**

  Die Oberfläche der Webkonsole für Central Manager wurde ansprechender gestaltet.

Zertifikate – Übersicht

Ein ***digitales Zertifikat*** ist eine verschlüsselte elektronische Datei, in der die Anmeldeinformationen eines Webservers oder Benutzers für Client-Server-Transaktionen festgelegt werden. Es gibt drei Arten von Zertifikaten, mit denen Sie Anmeldeinformationen festlegen und IVE-Transaktionen sichern können:

- ***Serverzertifikate***, die den Netzwerkverkehr zum und vom IVE sichern (Seite 69).
- ***Clientseitige Zertifikate***, die die Endbenutzer überprüfen. Clientseitige Zertifikate werden von den Browsern der Endbenutzer gesendet und dann von einem Stammzertifikat überprüft, das auf dem IVE installiert ist (Seite 70).
- ***Appletzertifikate***, auch als Codesignaturzertifikate bezeichnet, signieren die vom IVE vermittelten Applets erneut (Seite 71).

Außerdem können Endbenutzer mit einem Zertifikatserver authentifiziert werden. Ein ***Zertifikatserver*** ist mit den oben beschriebenen Lösungen vergleichbar, da Benutzer auf der Grundlage von Zertifikatattributen authentifiziert werden können. Die oben beschriebenen Zertifikatlösungen sind jedoch nur *Ergänzungen* zur Authentifizierung über einen Authentifizierungsserver, während ein Zertifikatserver Benutzer nur aufgrund ihrer Zertifizierungsattribute authentifiziert. Weitere Informationen finden Sie unter „Konfigurieren einer Zertifikatserverinstanz“ auf Seite 225.

Das IVE unterstützt X.509-Zertifikate, die mit DER, NET oder PEM (u.a. die Dateierweiterungen .cer, .crt, .der, .net und .pem) bzw. PKCS #12 (Dateierweiterungen u.a. .pfx und .p12) codiert sind.

Serverzertifikate

Das IVE verwendet ein temporäres, selbst signiertes digitales Zertifikat, das mit den bei der Initialisierung eingegebenen Daten lokal erstellt wird. Mithilfe dieses Serverzertifikats können die Benutzer sofort mit der Verwendung des IVE[1] beginnen.

1. Die Verschlüsselung für das während der Initialisierung erstellte selbst signierte Zertifikats ist zwar absolut sicher, für die Benutzer wird jedoch bei jeder Anmeldung am IVE eine Sicherheitswarnung angezeigt, da das Zertifikat nicht von einer Zertifizierungsstelle ausgestellt wurde.
Zu Produktionszwecken empfiehlt es sich, ein digitales Zertifikat von einer Zertifizierungsstelle zu beschaffen.

Wenn Sie nicht das selbst signierte Zertifikat des IVE verwenden möchten, können Sie ein digitales Zertifikat für das IVE mithilfe einer der folgenden Methoden beziehen:

- Ein vorhandenes Serverzertifikat und einen privaten Schlüssel auf den IVE importieren. Zunächst müssen Sie das Serverzertifikat und die private Schlüsseldatei vom vorhandenen Webserver exportieren. Anschließend importieren Sie diese Dateien über die Registerkarte **System > Configuration > Certificates > Server Certificate** (Seite 147).

  Wichtig: Beim Importieren eines Zertifikats muss dieses verschlüsselt sein, und das Kennwort muss mit dem Zertifikat exportiert werden. Außerdem können Sie können den privaten Schlüssel eines Webserverzertifikats nicht auf ein Access Series FIPS-Gerät importieren, da dieser Schlüssel in einer Umgebung erzeugt wird, die nicht mit FIPS kompatibel ist. Sie können aber einen Zertifikatsschlüssel zusammen mit der Security World von einem anderen NetScreen IVE Access Series-Gerät impotieren.

- Erstellen Sie eine Zertifikatssignaturanforderung (Certificate Signing Request, CSR), die an eine Zertifizierungsstelle gesendet wird (Seite 151). Wenn die Zertifizierungsstelle die signierte Datei zurücksendet, importieren Sie diese über die Registerkarte **System > Configuration > Certificates > Server Certificate** (Seite 152).

Clientzertifikate

Sie können das IVE so konfigurieren, dass ein Benutzer für die Anmeldung am System ein gültiges clientseitiges Zertifikat angeben muss. Um festzulegen, dass ein Benutzer ein gültiges clientseitiges Zertifikat angeben muss, müssen Sie die folgenden Schritte ausführen:

1. Installieren Sie ein clientseitiges Zertifikat über den Browser des Benutzers. Hilfe dazu können Sie den Anweisungen zu dem Browser entnehmen. Bei weiteren Fragen in diesem Zusammenhang lesen Sie die Ihrer IVE-Version entsprechenden Versionshinweise.
2. Auf der Registerkarte **System > Configuration > Certificates > CA Certificate** können Sie ein Stammzertifikat in das IVE importieren, das das clientseitige Zertifikat überprüft (Seite 153).

Wichtig: Das IVE unterstützt keine Zwischenserverzertifikate. Wenn Sie ein ***verkettetes Zertifikat***, d.h. ein vom Stammzertifikatsschlüssel signiertes Zwischenzertifikat, in das IVE importieren, importiert das IVE nur das erste Zertifikat. Wenn der Benutzer dann auf das IVE zugreifen möchte, wird eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. (Diese Warnung wird auch angezeigt, wenn der Benutzer ein Stammzertifikat in das IVE importiert, das nicht in den Browser des Benutzers eingebettet ist.) Beachten Sie jedoch, dass das VeriSign-Zwischenzertifikat in das IVE eingebettet ist. Wenn Sie den Stamm eines verketteten VeriSign-Serverzertifikats importieren, wird dem Benutzer daher keine Warnung vor einem nicht vertrauenswürdigen Zertifikat angezeigt.

3. Auf der Registerkarte **Users/Administrators > Authentication > Authentication Policy > Certificate** können Sie ein gültiges clientseitiges Zertifikat anfordern, um sich beim IVE anzumelden.
4. Sie können den Benutzerzugriff über die Menüseiten **Users** weiter einschränken:
   - **Authentication > Authentication Policy > Certificate**
   - **Roles > General > Restrictions > Certificate**

   Sie können auch den Administrator- und delegierten Administratorzugriff über die Menüseiten **Administrators** einschränken:
   - **Authentication > Authentication Policy > Certificate**
   - **Delegation > General > Restrictions > Certificate**

   Auf diesen Registerkarten können Sie X.509-DN-Attribute (Distinguished Name) angeben, die für die Authentifizierung erforderlich sind. Dies könnte beispielsweise erforderlich sein, wenn Sie dasselbe Zertifikat zwar für mehrere Rollen verwenden, den Zugriff auf eine bestimmte Ressource jedoch dadurch beschränken möchten, dass das Zertifikat eines Benutzers bestimmte DN-Attribute aufweisen muss.

Appletzertifikate

Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet mit einem eigenen Zertifikat neu, das nicht mit einem Standardstammzertifikat verkettet ist. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z.B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das NetScreen Instant Virtual Extranet zu vermittelnde Applets neu signiert.

Folgende Codesignaturzertifikate werden unterstützt:

- **Microsoft Authenticode-Zertifikat**

  Mit diesem Zertifikat signiert das IVE Applets, die über MS JVM oder SUN JVM ausgeführt werden. Beachten Sie, dass nur von Verisign ausgestellte Microsoft Authenticode-Zertifikate unterstützt werden.

- **JavaSoft-Zertifikat**

  Mit diesem Zertifikat signiert das IVE Applets, die über SUN JVM ausgeführt werden.

Beachten Sie bei der Auswahl des zu importierenden Codesignaturzertifikats folgende Browserabhängigkeiten:

- **Internet Explorer**

  Auf neuen Computern, auf denen bei der Lieferung Windows XP vorinstalliert ist, wird in Internet Explorer normalerweise die SUN JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

  Auf PCs unter Windows 98 oder 2000 oder auf PCs, die auf Windows XP aktualisiert wurden, wird in Internet Explorer normalerweise die MS JVM ausgeführt. Dies bedeutet, dass Applets vom IVE mit einem Authenticode-Zertifikat neu signiert werden müssen.

- **Netscape**

  Netscape-Browser unterstützen nur die SUN JVM. Dies bedeutet, dass Applets vom IVE mit dem JavaSoft-Zertifikat neu signiert werden müssen.

Weitere Hinweise für Benutzer der SUN JVM:

- Standardmäßig werden Applets vom Java-Plug-In zusammen mit dem Codesignaturzertifikat zwischengespeichert, das beim Benutzerzugriff auf das Applet bereitgestellt wird. Der Browser stellt Applets also auch nach dem Importieren eines Codesignaturzertifikats in das IVE weiterhin mit dem ursprünglichen Zertifikat bereit. Um sicherzustellen, dass Benutzer der SUN JVM keine Aufforderungen für nicht vertrauenswürdige Zertifikate für Applets erhalten, auf die sie vor dem Import eines Codesignaturzertifikats zugegriffen haben, muss der Cache des Java-Plug-Ins geleert werden. Benutzer können den Cache auch deaktivieren. Dies kann jedoch die Leistung beeinträchtigen, da das Applet bei jedem Benutzerzugriff abgerufen werden muss.
- Das Java-Plug-In verwaltet eine eigene Liste vertrauenswürdiger Webserverzertifikate, die sich von der entsprechenden Liste des Browsers unterscheidet. Wenn ein Benutzer auf ein Applet zugreift, stellt die SUN JVM (zusätzlich zum Browser) eine eigene Verbindung mit dem Webserver her, auf dem sich das Applet befindet. Dem Benutzer bietet

sich dann die Möglichkeit, zusätzlich zum Codesignaturzertifikat das Webserverzertifikat anzunehmen. In solchen Fällen muss der Benutzer die Schaltfläche **Always Trust** für das Webserverzertifikat auswählen. Wenn der Benutzer bei der Auswahl dieser Schaltfläche für das Webserverzertifikat zu lange wartet, wird das Applet aufgrund einer voreingestellten Höchstzeitdauer im Java-Plug-In nicht geladen.

Cluster – Übersicht

Secure Access Series und Secure Access FIPS Series unterstützen verschiedene Clusterkonfigurationen. Ein ***Clusterpaar*** besteht aus zwei Access 1000-, 3000- oder 5000-Plattformen, die über ein LAN oder WAN in einer Aktiv/Passiv- oder Aktiv/Aktiv-Konfiguration bereitgestellt werden, um hohe Verfügbarkeit und Lastenausgleich zu gewährleisten. Ein ***Cluster aus mehreren Einheiten*** besteht aus zwei oder mehr Access 5000-Plattformen, die über ein LAN oder WAN in einer Aktiv/Passiv-[1] oder Aktiv/Aktiv-Konfiguration bereitgestellt werden, um bessere Skalierbarkeit, hohe Verfügbarkeit und höhere Leistung zu gewährleisten.

In diesem Abschnitt erhalten Sie eine Übersicht über Cluster. Informationen zur Vorgehensweise finden Sie unter:

Definieren und Initialisieren eines Clusters 168
Hinzufügen eines IVE zu einem Cluster über die Webkonsole 176
Hinzufügen eines IVE zu einem Cluster über die serielle Konsole 179
Angeben eines neuen Clustermitglieds 170
Verwalten von Netzwerkeinstellungen für Clusterknoten 172
Ändern von Clustereigenschaften oder Löschen eines Clusters 182
Aktualisieren des Dienstpakets für Clusterknoten 173

Cluster – Übersicht

Sie legen einen Cluster in einem IVE mithilfe der folgenden drei Angaben fest:

1. Eine Bezeichnung für den Cluster
2. Ein gemeinsames Kennwort für die Clustermitglieder
3. Einen Namen, der das IVE im Cluster kennzeichnet

Nachdem Sie diese Daten auf der Registerkarte **System > Clustering > Create** angegeben haben, klicken Sie auf **Create Cluster**, um den Cluster zu initiieren und das aktuelle IVE zum Cluster hinzuzufügen. Nach dem Definieren des Clusters werden auf der Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt. Die Registerkarte **Status** enthält den Clusternamen und -typ, ermöglicht Ihnen die Angabe neuer Mitglieder sowie die Verwaltung bestehender Mitglieder und bietet umfassende Informationen zum Clusterstatus.

1. Ein Cluster mit mehreren Einheiten ist nur als Clusterpaar im Aktiv/Passiv-Modus verfügbar.

Nach der Definition und Initialisierung eines Clusters müssen Sie angeben, welche IVEs dem Cluster hinzugefügt werden. Nachdem ein IVE als vorgesehenes Mitglied angegeben wurde, können Sie es dem Cluster über folgende Komponenten hinzufügen:

- **Webkonsole**

  Wenn ein konfiguriertes IVE als eigenständiges Gerät betrieben wird, können Sie es über seine Webkonsole zu einem Cluster hinzufügen.

- **Serielle Konsole**

  Ein werksseitig eingestelltes IVE können Sie über seine serielle Konsole zu einem Cluster hinzufügen, indem Sie bei der Ersteinrichtung die Minimalinformationen eingeben.

Wenn ein IVE einem Cluster hinzugefügt wird, initialisiert es seinen Status von einem vorhandenen Mitglied, das Sie angeben. Das neue Mitglied sendet eine Nachricht an das vorhandene Mitglied und fordert die Synchronisierung an. Das bestehende Mitglied sendet daraufhin den Systemstatus an das neue Mitglied, wodurch *alle* Systemdaten dieses Geräts überschrieben werden. Wenn sich zu einem späteren Zeitpunkt bei einem der Clustermitglieder der Status ändert, synchronisieren die Clustermitglieder die Daten. Die Kommunikation zwischen Clustermitgliedern ist verschlüsselt, um Angriffe von außerhalb der firmeninternen Firewall zu verhindern. Jedes IVE verwendet das gemeinsame Kennwort zum Entschlüsseln der Nachrichten von anderen Clustermitgliedern. Das Clusterkennwort wird aus Sicherheitsgründen nicht über die IVEs hinweg synchronisiert. Bei der Synchronisierung empfängt der neue Knoten das Dienstpaket, das den Knoten aktualisiert, sofern auf diesem noch ein älteres Dienstpaket ausgeführt wird.

Weitere Informationen finden Sie unter:

Bereitstellen eines Clusterpaars im Aktiv/Passiv-Modus 76
Bereitstellen eines Clusterpaars oder eines Clusters mit mehreren Einheiten im Aktiv/Aktiv-Modus 78
Statussynchronisierung 79
Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung 81

Bereitstellen eines Clusterpaars im Aktiv/Passiv-Modus

Die NetScreen Access 1000-, 3000- und 5000-Plattformen können als Clusterpaar im Aktiv/Passiv-Modus bereitgestellt werden. In diesem Modus bearbeitet ein IVE aktiv Benutzeranforderungen, während das andere IVE passiv im Hintergrund ausgeführt wird, um Statusdaten, einschließlich Systemstatus, Benutzerprofil und Protokollmeldungen, zu synchronisieren. Benutzeranforderungen an die Cluster-VIP werden an das aktive IVE gelei-

tet. Wird das aktive IVE offline geschaltet, beginnt das Standby-IVE automatisch mit der Bearbeitung der Benutzeranforderungen. Die Benutzer müssen sich nicht neu anmelden. IVE-Sitzungsdaten, die ein paar Sekunden vor der Offline-Schaltung des aktiven Geräts eingegeben wurden, beispielsweise Cookies und Kennwörter, werden jedoch möglicherweise nicht in das aktuelle IVE-Feld synchronisiert. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

Die folgende Abbildung zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Passiv mit zwei IVEs, für die externe Ports aktiviert sind. Dieser Modus erhöht zwar weder den Durchsatz noch die Benutzerkapazität, bietet jedoch Redundanz, um auf unerwartete Systemausfälle zu reagieren.

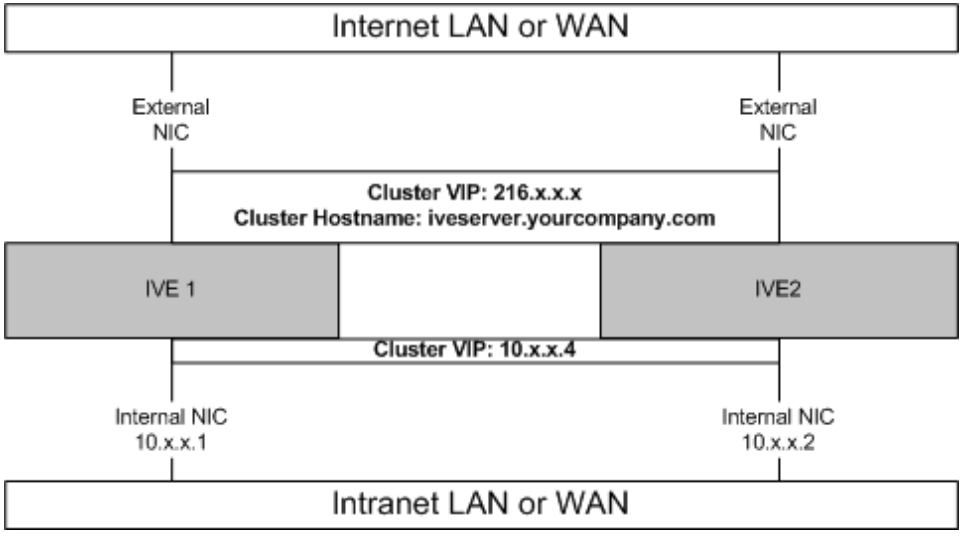


Abbildung 4: Aktiv/Passiv-Clusterpaar
Die Abbildung zeigt einen Aktiv/Passiv-Cluster innerhalb des Netzwerks. IVE-Benutzeranforderungen werden an die Cluster-VIP geleitet, die diese dann an das aktive IVE weiterleitet.

Bereitstellen eines Clusterpaars oder eines Clusters mit mehreren Einheiten im Aktiv/Aktiv-Modus

Die NetScreen Access 1000-, 3000- und 5000-Plattformen können als Clusterpaar im Aktiv/Aktiv-Modus bereitgestellt werden.

Im Aktiv/Aktiv-Modus verarbeiten alle IVEs im Cluster aktiv die Benutzeranforderungen, die von einem externen Load-Balancer oder nach dem Rotationsprinzip über DNS gesendet wurden. Der Load-Balancer hostet die Cluster-VIP und leitet Benutzeranforderungen auf der Grundlage von SIP-Weiterleitung (Source IP) an ein in seiner Clustergruppe definiertes IVE weiter. Wenn ein IVE offline geschaltet wird, verteilt der Load-Balancer die Datenlast auf den aktiven IVEs um. Die Benutzer müssen sich nicht neu anmelden. IVE-Sitzungsdaten, die ein paar Sekunden vor der Offline-Schaltung des aktiven Geräts eingegeben wurden, beispielsweise Cookies und Kennwörter, werden jedoch möglicherweise nicht in das aktuelle IVE-Feld synchronisiert. In diesem Fall müssen sich die Benutzer an den Back-End-Webservern neu anmelden.

Der IVE-Cluster selbst führt keine automatischen Failover- oder Lastenausgleichoperationen durch. Er synchronisiert jedoch Statusdaten (System-, Benutzer- und Protokolldaten) zwischen den Clustermitgliedern. Wenn ein offline geschaltetes IVE wieder online geschaltet wird, passt der Load-Balancer die Datenlast erneut an, um sie auf alle aktiven Mitglieder zu verteilen. Dieser Modus bietet gesteigerten Durchsatz und höhere Leistung während Spitzenlastzeiten, verbessert jedoch die Skalierbarkeit über die Gesamtzahl der lizenzierten Benutzer hinaus nicht.

Das IVE hostet eine HTML-Seite, die den Dienststatus für jedes IVE in einem Cluster zur Verfügung stellt. Externe Load-Balancer können anhand dieser Ressource ermitteln, wie die Datenlast effektiv auf die Clusterknoten verteilt werden kann.

Der L7-Überprüfungs-URL lautet:

https://<IVE-Hostname>/dana-na/healthcheck/healthcheck.cgi

Die folgende Abbildung zeigt eine IVE-Clusterkonfiguration vom Typ Aktiv/Aktiv, bei der externe Ports für die IVEs aktiviert sind.

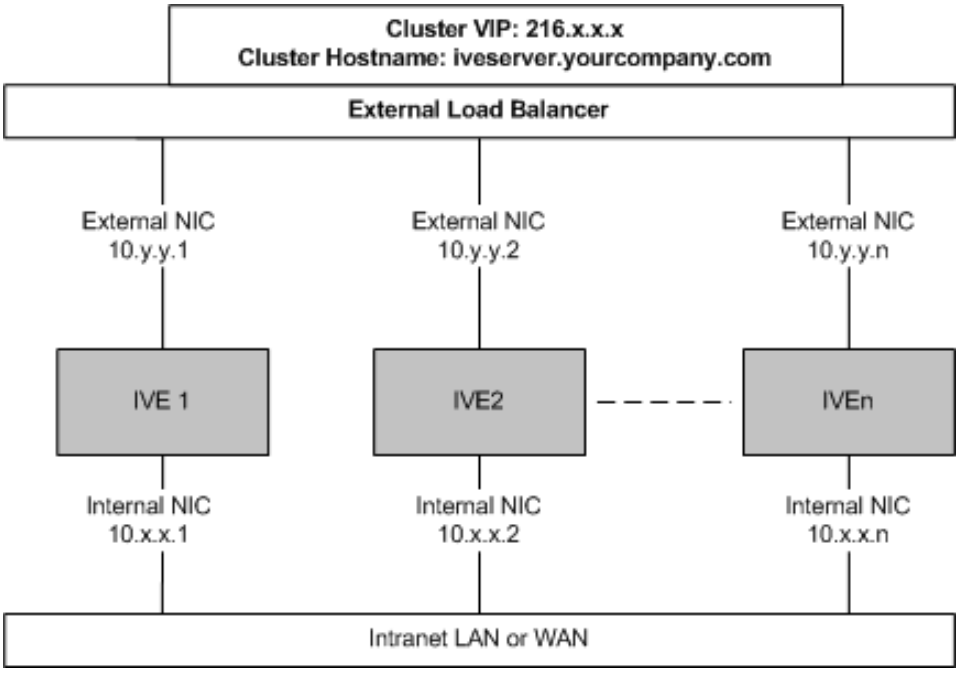


Abbildung 5: Aktiv/Aktiv-Konfiguration
Diese Abbildung zeigt eine Aktiv/Aktiv-Clusterkonfiguration, die hinter einem externen Load-Balancer bereitgestellt wird. Sie können ein Clusterpaar oder ein Cluster mit mehreren Einheiten im Aktiv/Aktiv-Modus bereitstellen. IVE-Benutzeranforderungen werden an die Cluster-VIP geleitet, die auf dem Load-Balancer festgelegt wurde, der sie an das entsprechende Gerät weiterleitet.

Statussynchronisierung

Die Synchronisierung des IVE-Status erfolgt nur über die internen Netzwerkkarten, daher muss jedes Clustermitglied das Clusterkennwort besitzen, um mit anderen Mitgliedern kommunizieren zu können. Die Clustermitglieder synchronisieren Daten, wenn bei einem der Mitglieder des Clusters eine Statusänderung erfolgt. IVE-Clusterstatusdaten sind entweder ***permanent***, d.h. dauerhaft im IVE gespeichert, oder ***temporär***, d.h. nur für die Dauer der Benutzersitzung im IVE gespeichert. IVE-Statusdaten werden in die folgenden Hauptkategorien unterteilt:

- **Systemstatus** – Dieser Status ist permanent und ändert sich nicht häufig.
  - Netzwerkeinstellungen
  - Authentifizierungsserver-Konfiguration
  - Konfiguration von Autorisierungsgruppen, zum Beispiel Zugriffssteuerungsliste, Lesezeichen, Nachrichtenübermittlung und Anwendungsdaten
- **Benutzerprofil** – Diese Daten können permanent oder temporär sein, je nachdem, ob beständige Cookies und permanente Kennwortzwischenspeicherung aktiviert sind. Wenn keine dieser Funktionen aktiviert ist, sind die Daten temporär und fallen in die nächste Kategorie.
  - Benutzerlesezeichen – permanent
  - Permanente Benutzercookies – Wenn die Funktion für permanente Cookies aktiviert ist, speichert das IVE Benutzercookies für Websites, die permanente Cookies ausgeben.
  - Permanente Benutzerkennwörter – Wenn die Funktion zum Zwischenspeichern von Kennwörtern aktiviert ist, können Benutzer festlegen, dass ihre Anmeldeinformationen für Anwendungen und Websites gespeichert werden.
- **Benutzersitzung** – Dieser Status ist temporär und dynamisch. Die Benutzersitzungsdaten umfassen Folgendes:
  - Das IVE-Sitzungscookie des Benutzers
  - Temporäre Benutzerprofildaten, zu denen Cookies und Kennwörter zählen, die nur während der Benutzersitzung gespeichert werden.
- **Überwachungstatus** – Dieser permanente Status ist dynamisch und besteht aus Protokollmeldungen[1].

Das IVE ist für die Synchronisierung von Daten zwischen Clustermitgliedern verantwortlich, unabhängig davon, ob Sie einen Cluster im Aktiv/Passiv-Modus oder im Aktiv/Aktiv-Modus bereitstellen. Das IVE synchronisiert alle Systemdaten, Benutzerprofildaten und das IVE-Benutzersitzungscookie sofort. Wenn ein Clustermitglied offline geschaltet wird, müssen sich die Benutzer daher nicht erneut am IVE anmelden. Wenn das IVE Benutzersitzungsprofile synchronisiert und Statusdaten überwacht, tritt eine geringfügige Latenz auf. Falls ein Mitglied offline geschaltet wird, kann es passieren, dass sich der Benutzer bei manchen Back-End-Webanwendungen anmelden muss und Administratoren keinen Zugriff auf die Protokolle auf dem ausgefallenen Computer haben.

Sie können auch Synchronisierungseinstellungen konfigurieren, um die Leistung zu verbessern:

1. Wenn Sie ein IVE zu einem Cluster hinzufügen, sendet der Clusterleiter keine Protokollmeldungen an das neue Mitglied. Protokollmeldungen werden nicht zwischen Clustermitgliedern synchronisiert, wenn ein Mitglied seinen Dienst wieder aufnimmt oder ein offline geschaltetes IVE wieder online geschaltet wird. Sobald alles IVEs online sind, werden die Protokollmeldungen jedoch synchronisiert.

- **Angeben des Synchronisierungsprotokolls**

  Wenn Sie drei oder mehr IVEs in einen Cluster mit mehreren Einheiten oder mehreren Sites betreiben, können Sie das Synchronisierungsprotokoll auswählen, das der Konfiguration Ihrer Netzwerkhardware am besten entspricht:

  - **Unicast**

    Das IVE sendet an alle Knoten im Cluster die gleiche Meldung. (Dies ist das einzige Synchronisierungsprotokoll, das für Cluster mit zwei Knoten und Multisite-Cluster verfügbar ist.)

  - **Multicast**

    Das IVE sendet eine Meldung an alle Clusterknoten im Netzwerk.

  - **Broadcast**

    Das IVE sendet eine Meldung an alle Geräte im Netzwerk, wobei nicht zum Cluster gehörige Knoten die Meldung löschen.

Hinweis: Die auf der Cluster-Eigenschaftenseite konfigurierte Einstellung für die Datenübertragung wird nur von den Mitgliedern derselben Site (desselben Subnetzwerks) verwendet. Beispielsweise können Sie in einer Cluster-Site mit 4 Knoten die Multicast-Synchronisierungsmethode festlegen. Die betreffende Site kann jedoch nur mit Sites kommunizieren, die die Unicast-Methode anwenden.

- **Angeben, ob Protokollmeldungen synchronisiert werden sollen**

  Protokollmeldungen können zu umfangreicher Belastung des Netzwerks führen und die Clusterleistung beeinträchtigen. Wir empfehlen, diese Option zu deaktivieren, insbesondere bei einer Multi-Unit-Konfiguration.

Bereitstellen eines Clusters in einer Access Series FIPS-Umgebung

Neben der Freigabe von Status-, Benutzerprofil-, Benutzersitzungs- und Überwachungsstatusdaten können Mitglieder eines Access Series FIPS-Clusters auch Security World-Daten gemeinsam nutzen. Alle Clustermitglieder verwenden gemeinsam denselben privaten Schlüssel, und sie sind über dieselben Administratorkarten zugänglich. Da für das Ändern einer Security World der physische Zugriff auf ein Kryptographiemodul erforderlich ist, können Access Series FIPS-Clustermitglieder jedoch nicht alle ihre Daten im Rahmen des standardmäßigen IVE-Synchronisierungsvorgangs freigeben. Stattdessen muss zum Erstellen eines Access Series FIPS-Clusters Folgendes ausgeführt werden:

1. **Erstellen Sie einen Cluster von Access Series FIPS-Geräten über die Webkonsole.**

   Wie bei einem standardmäßigen IVE-Cluster wird jeder Clusterknoten in einem Access Series FIPS-Cluster mit den Systemstatusdaten vom angegebenen Clustermitglied initialisiert, wobei alle vorhandenen Daten auf dem Knotengerät überschrieben werden.

2. **Aktualisieren Sie die Security World auf jedem Gerät manuell.**

   Nach dem Erstellen eines Clusters müssen Sie jeden Clusterknoten mit der Security World des angegebenen Mitglieds initialisieren. Dazu verwenden Sie eine Administratorkarte, die bereits für die Security World initialisiert ist, einen Smartcardleser und die serielle Konsole.

Anweisungen hierfür finden Sie unter „Hinzufügen eines IVE zu einem Cluster über die Webkonsole“ auf Seite 176.

Wenn Sie eine vorhandene Security World in einem Cluster ändern möchten, müssen Sie das Kryptographiemodul der einzelnen Clustermitglieder mithilfe einer Administratorkarte, eines Smartcardlesers und der seriellen Konsole des IVE aktualisieren. Anweisungen hierfür finden Sie unter „Anhang D: “ auf Seite 453.

Delegierte Administration – Übersicht

Das IVE-Zugriffsverwaltungssystem ermöglicht das Delegieren verschiedener IVE-Verwaltungsaufgaben an verschiedene Administratoren mithilfe von Administratorrollen[1]. Eine ***Administratorrolle*** ist eine Einheit, die Verwaltungsfunktionen und Sitzungseigenschaften des IVE für Administratoren angibt, die der Rolle zugeordnet sind. Sie können eine Administratorrolle anpassen, indem Sie Merkmalssätze und Benutzerrollen für das IVE auswählen, die Mitglieder der Administratorrolle anzeigen und verwalten dürfen.

Sie können z.B. eine Administratorrolle mit der Bezeichnung „Helpdesk-Administratoren" erstellen und dieser Rolle Benutzer zuweisen, die für die Annahme von Supportfragen der Ebene 1 verantwortlich sind. Dazu gehört z.B. der Support für Benutzer, die nicht auf eine Webanwendung oder IVE-Seite zugreifen können. Für die Problembehebung können die Einstellungen für die Rolle „Helpdesk-Administratoren" wie folgt vorgenommen werden.

- Gewähren Sie den Helpdesk-Administratoren Schreibzugriff auf die Seite **System > Log/Monitoring**, damit sie IVE-Protokolle anzeigen und filtern, kritische Ereignisse in einzelnen Sitzungsverläufen verfolgen und die Seite **Maintenance > Troubleshooting** anzeigen und somit die Probleme auf einzelnen Benutzersystemen aufspüren können.
- Gewähren Sie den Helpdesk-Administratoren Lesezugriff auf die Seiten **User > Roles**, damit sie darüber informiert sind, welche Lesezeichen, Freigaben und Anwendungen den individuellen Benutzerrollen zur Verfügung stehen und sie außerdem die Seiten **Resource Policy** und somit die Richtlinien anzeigen können, die einzelnen Benutzern den Zugriff auf ihre Lesezeichen, Freigaben und Anwendungen verweigern.
- Verweigern Sie den Helpdesk-Administratoren Zugriff auf die restlichen Seiten **System** und **Maintenance**, die hauptsächlich zum Konfigurieren von Systemeinstellungen (Installation von Lizenzen und Dienstpaketen) und nicht zur Behebung von einzelnen Benutzerproblemen verwendet werden.

Verwenden Sie die Einstellungen auf der Seite **Administrators > Delegation** (Seite 265), um andere Administratorrollen zu erstellen und deren Zugriff auf die Webkonsole anzupassen.

1. Neben evtl. von Ihnen erstellten delegierten Administratorrollen, verfügt das IVE über zwei Grundtypen von Administratoren: Superadministratoren (.Administrators role), die alle Administrationsaufgaben über die Webkonsole ausführen dürfen, und Administratoren mit Lesezugriff (.Read-only Administrators role), die die gesamte IVE-Konfiguration auf der Webkonsole anzeigen, jedoch nicht ändern dürfen. Superadministratoren und Administratoren mit Lesezugriff sind in allen IVE-Produkten verfügbar.

E-Mail-Client – Übersicht

Die vom IVE bereitgestellte E-Mail-Unterstützung hängt von den optionalen Funktionen ab, die für den IVE-Server lizenziert sind:

- **Secure Email Client Aktualisierungsoption**

  Wenn Sie über die Aktualisierungsoption Secure Email Client verfügen, unterstützt das IVE IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol). Sie können den Zugriff auf die IMAP/POP/SMTP-Mailserver der Firma ganz einfach aktivieren, indem Sie den Mailserver, die E-Mail-Sitzung und die Authentifizierungsinformationen auf der Seite **Resource Policies > Email Settings** (Seite 379) angeben.

- **Secure Application Manager Aktualisierungsoption**

  Wenn Sie über die Aktualisierungsoption Secure Application Manager verfügen, unterstützt das IVE das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll. Sie können den Zugriff auf Microsoft Exchange Server und Lotus Notes Server auf der Seite **User > Roles >SAM > Applications** (Seite 304) aktivieren.

  Wichtig: Wenn der IVE-Server mit der Aktualisierungsoption **Secure Application Manager** lizenziert ist, die das systemeigene MAPI-Protokoll von Microsoft Exchange und das systemeigene Lotus Notes-Protokoll unterstützt, trifft dieser Abschnitt nicht zu.

Die Aktualisierungsoption Secure Email Client bietet Benutzern die Möglichkeit, mit standardbasierten E-Mail-Clients sicher von Remotestandorten auf firmeninterne E-Mail-Nachrichten zuzugreifen, ohne dass weitere Software (z.B. ein VPN-Client) benötigt wird. Der IVE-Server funktioniert mit jedem Mailserver, der IMAP4 (Internet Mail Application Protocol), POP3 (Post Office Protocol) und SMTP (Simple Mail Transfer Protocol) unterstützt. Hierzu zählen auch Microsoft Exchange Server und Lotus Notes Mail Server, die IMAP4/POP3/SMTP-Schnittstellen zur Verfügung stellen.

Der IVE-Server befindet sich zwischen dem Remoteclient und dem Mailserver und fungiert als sicherer E-Mail-Proxy. Der Remoteclient verwendet den IVE-Server als (virtuellen) Mailserver und sendet E-Mail über das SSL-Protokoll. Der IVE-Server beendet SSL-Verbindungen des Clients und leitet den entschlüsselten E-Mail-Verkehr innerhalb des LAN an den Mailserver weiter. Der IVE-Server wandelt den unverschlüsselten Datenverkehr des Mailservers dann in S-IMAP (Secure IMAP)-, S-POP (Secure POP)- und S-SMTP (Secure SMTP)-Datenverkehr um und sendet ihn über SSL an den E-Mail-Client.

Weitere Informationen finden Sie unter:

Auswählen eines E-Mail-Clients 86
Arbeiten mit einem standardbasierten Mailserver 86
Arbeiten mit Microsoft Exchange Server 87
Arbeiten mit Lotus Notes und Lotus Notes Mail Server 90

Auswählen eines E-Mail-Clients

Das IVE unterstützt die folgenden E-Mail-Clients:

- Outlook 2000 und 2002
- Outlook Express 5.5 und 6.x
- Netscape Messenger 4.7x und Netscape Mail 6.2

Benutzer, die Remotezugriff auf E-Mail-Nachrichten benötigen, können normalerweise in zwei Kategorien eingeteilt werden:

- **Laptopbenutzer in der Firma**

  Diese Benutzer verwenden im Büro und unterwegs das gleiche Laptop.
- **Benutzer mit Heimcomputern**

  Diese Benutzer verwenden zu Hause einen anderen Computer als im Büro.

Bevor Sie Benutzern einen E-Mail-Client empfehlen, sollten Sie die folgenden Abschnitte lesen, in denen erläutert wird, wie die unterstützten Clients mit folgenden Komponenten interagieren:

- Standardbasierte Mailserver wie Lotus Notes Mail Server (Seite 86)
- Microsoft Exchange Server (Seite 87)

Hinweis: Anleitungen zum Konfigurieren der unterstützten E-Mail-Clients finden Sie auf der NetScreen-Supportsite unter folgender Adresse: http://support.netscreen.com.

Arbeiten mit einem standardbasierten Mailserver

Das IVE funktioniert mit Mailservern, die IMAP4, POP3 und SMTP unterstützen.

IMAP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können jeden der sechs unterstützen E-Mail-Clients verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den IVE-Server verweist.
- **Benutzer mit Heimcomputern:**Diese Benutzer können für den Remotezugriff auf den IMAP-Server über das IVE jeden der sechs unterstützten E-Mail-Clients verwenden.

POP-Mailserver

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der vier Outlook-E-Mail-Clients* verwenden. Wir empfehlen, im Büro und unterwegs den gleichen Client zu verwenden, um übergangsloses Arbeiten zu ermöglichen. Der Client muss dabei so konfiguriert sein, dass er auf den IVE-Server verweist.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf den POP-Server über das IVE einen der vier Outlook-E-Mail-Clients* verwenden.

*Netscape-E-Mail-Clients können im POP-Modus nicht für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll ist jedoch für den IVE-Server für die sichere Datenübertragung erforderlich.

Arbeiten mit Microsoft Exchange Server

Der Microsoft Exchange Server unterstützt:

- Systemeigene MAPI-Clients (Messaging Application Programming Interface)
- IMAP-Clients
- POP-Clients
- Outlook Web Access (OWA)

Der IVE-Server bietet Zugriff auf Microsoft Exchange Server über IMAP- und POP-Clients anhand der Aktualisierungsoption Secure Email Client und über OWA anhand der Funktion für sicheres Webbrowsing.

Wenn Sie den Zugriff auf Microsoft Exchange Server über das systemeigene MAPI-Protokoll ermöglichen möchten, muss das IVE mit der Aktualisierungsoption Secure Application Manager lizenziert sein.

Exchange Server und IMAP-Clients

Falls es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können einen der Outlook Express- oder Netscape-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden.[1]
- **Benutzer mit Heimcomputern:** Diese Benutzer können einen der sechs unterstützten E-Mail-Clients für den Remotezugriff auf Exchange Server über das IVE verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

Wenn Benutzer die Outlook Express- oder Netscape-Clients im IMAP-Modus ausführen, beachten Sie bitte das folgende Verhalten bei der Ordnerverwaltung:

- **Bei Verwendung von Outlook Express-E-Mail-Clients**

  Gelöschte E-Mail-Nachrichten werden im Posteingang von Outlook Express durchgestrichen angezeigt. Sie werden nicht in den Ordner **Gelöschte Objekte** auf dem Exchange Server verschoben, wie es bei Verwendung des Outlook 2000- oder 2002-Clients der Fall ist. Wenn ein Benutzer gelöschte E-Mail-Nachrichten in einem Outlook Express-Client entfernt, werden die E-Mail-Nachrichten endgültig gelöscht. Wir empfehlen Benutzern von Outlook Express die folgende Vorgehensweise:
  - Zu löschende E-Mail-Nachrichten sollten manuell in den unter **Lokale Ordner** angeordneten Ordner **Gelöschte Objekte** verschoben werden (hierbei handelt es sich um Standardordner). Dieser Ordner wird mit dem Ordner **Gelöschte Objekte** auf dem Exchange Server synchronisiert, sodass Benutzer gelöschte E-Mail-Nachrichten später abrufen können.
  - Sie sollten die gelöschten E-Mail-Nachrichten zunächst im Posteingang von Outlook Express lassen und sie dann bei der nächsten Anmeldung bei Outlook 2000 oder 2002 in den Ordner **Gelöschte Objekte** verschieben.
- **Bei Verwendung von Netscape-E-Mail-Clients**

  Gelöschte E-Mail-Nachrichten werden in den Papierkorbordner von Netscape verschoben und im Posteingang von Netscape nicht mehr an-

1. Der Outlook 2000-Client unterstützt nur eine Mailserverkonfiguration, in diesem Fall den systemeigenen MAPI-Modus. Dies verhindert, dass Benutzer den gleichen Client für den Remotezugriff verwenden. Der Outlook 2002-Client bietet Unterstützung für gleichzeitige MAPI- und IMAP-Serverkonfigurationen. Er unterstützt jedoch keinen IMAP-Zugriff, wenn das MAPI-Konto offline ist, und verhindert hierdurch, dass Remotebenutzer E-Mail-Nachrichten abrufen können.

gezeigt. Aus dem Posteingang von Outlook 2000 oder 2002 werden sie jedoch erst dann entfernt, wenn die Benutzer folgendermaßen vorgehen:

1. Konfigurieren Sie Netscape so, dass gelöschte Nachrichten in den Papierkorbordner verschoben werden, und aktivieren Sie die Option zum Leeren des Posteingangs bei Beendigung des Programms.
2. Sie sollten immer nur eines der Programme ausführen und schließen, wenn Sie Ihre Arbeit beendet haben. Der Posteingang des anderen Programms wird dann mit dem Server synchronisiert, sodass die gleichen Nachrichten angezeigt werden.

Gesendete E-Mail-Nachrichten werden außerdem in den Netscape-Ordner für gesendete Objekte (oder einen anderen benutzerdefinierten Ordner) verschoben. Wenn Benutzer möchten, das gesendete Nachrichten im Ordner **Gesendete Objekte** von Microsoft Exchange Server angezeigt werden, müssen sie sie manuell aus dem Netscape-Ordner für gesendete Objekte in den Ordner **Gesendete Objekte** ziehen.

Exchange Server und POP-Clients

Wenn es sich bei dem firmeneigenen Mailserver um Exchange Server handelt, ist der Bürocomputer eines Mitarbeiters wahrscheinlich für die Verwendung des E-Mail-Clients Outlook 2000 oder 2002 im systemeigenen MAPI-Modus konfiguriert.

- **Laptopbenutzer in der Firma:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der unterstützten Outlook Express-Clients* verwenden.
- **Benutzer mit Heimcomputern:** Diese Benutzer können für den Remotezugriff auf Exchange Server über das IVE einen der vier Outlook-Clients* verwenden, wobei davon ausgegangen wird, dass auf dem Remotecomputer kein MAPI-Konto konfiguriert ist.

*Netscape-E-Mail-Clients können im POP-Modus nicht für den Remotezugriff verwendet werden, da sie S-POP nicht unterstützen. Dieses Protokoll ist jedoch für den IVE-Server für die sichere Datenübertragung erforderlich.

Exchange Server und Outlook Web Access

Um auf dem Exchange-Server OWA-Zugriff zur Verfügung zu stellen und es Benutzern zu ermöglichen, über die Webbrowsingfunktion des IVE auf den Exchange-Server zuzugreifen, müssen Sie OWA lediglich im Intranet als Webanwendung bereitstellen. Es ist keine weitere Einrichtung erforderlich, um eine OWA-Implementierung außerhalb des Netzwerks bereitzustellen.

Hinweis: Bei Verwendung des IVE-Servers für den Zugriff auf Outlook Web Access wird der IIS-Webserver für OWA vor Standardangriffen (z.B. Nimda) geschützt und bietet daher erheblich höhere Sicherheit als der Einsatz von OWA direkt über das Internet.

Arbeiten mit Lotus Notes und Lotus Notes Mail Server

Der Lotus Notes Mail Server stellt POP3- und IMAP4-Schnittstellen zur Verfügung, sodass Benutzer E-Mail von einer Lotus Notes-Mailkonfiguration über das IVE abrufen können. Um zu ermitteln, welcher E-Mail-Client sich für die E-Mail-Benutzer im Unternehmen empfiehlt, die Remotezugriff auf den Lotus-Mailserver benötigen, lesen Sie den Abschnitt über die Arbeit mit standardbasierten Mailservern, „Arbeiten mit einem standardbasierten Mailserver“ auf Seite 86.

Hostprüfung – Übersicht

Hostprüfung ist ein clientseitiger Agent, der Endpunktsicherheitsprüfungen an Hosts durchführt, die mit dem IVE eine Verbindung herstellen. Sie können die Hostprüfung aufrufen, bevor Sie einem Benutzer eine IVE-Anmeldeseite anzeigen lassen und wenn die Rollenzuordnungsregel oder Ressourcenrichtlinie ausgewertet wird. Das IVE kann die Eigenschaften für die Endpunktsicherheit auf Hosts mithilfe der folgenden Verfahren überprüfen:

- **Implementierung der NetScreen Hostprüfung einer unterstützten Anwendung für die Endpunktsicherheit**

  Das ActiveX-Steuerelement ruft die Integration der NetScreen Hostprüfung des angegebenen Endpunktsicherheitsprodukts eines Drittanbieters auf und untersucht den Rückgabewert, um festzustellen, ob das Produkt entsprechend den konfigurierten Richtlinien ausgeführt wird. Das IVE unterstützt gegenwärtig die nahtlose Integration der NetScreen Hostprüfung mit folgenden Produkten:

  - Sygate Enforcement API
  - Sygate Security Agent
  - Zone Labs: ZoneAlarm Pro und Zone Labs Integrity
  - McAfee Desktop Firewall 8.0
  - InfoExpress CyberGatekeeper Agent

- **NetScreen Hostprüfung Integration anhand einer benutzerdefinierten DLL**

  Die NetScreen Hostprüfungs-API ermöglicht Ihnen das Schreiben einer DLL, die benutzerdefinierte clientseitige Überprüfungen ausführt. Sie müssen diese DLL auf jedem Clientcomputer installieren. Die Dokumentation zur NetScreen Hostprüfung-API ist verfügbar auf der Supportsite: http://support.netscreen.com.

- **Attributüberprüfung**

  Das ActiveX-Steuerelement sucht nach den Spuren der angegebenen Anwendung, einschließlich Prozessen, Dateien und Registrierungseinträgen.

Erstellen globaler Richtlinien für die Hostprüfung

Um die Hostprüfung zum Durchsetzen von Richtlinien für die Verwaltung von Endpunktsicherheit verwenden zu können, müssen Sie globale Richtlinien für die Hostprüfung erstellen, die Folgendes angeben:

- **Hostüberprüfungsmethoden**

  Eine ***Methode*** ist die Implementierung der NetScreen Hostprüfung eines Endpunktsicherheitsprodukts von einem Drittanbieter, das ermittelt, ob eine Anwendung entsprechend den konfigurierten Richtlinien ausgeführt wird. Gegenwärtig bietet die Hostprüfung Methoden für folgende Produkte:

  - Sygate Enforcement API
  - Sygate Security Agent
  - Zone Labs: ZoneAlarm Pro und Zone Labs Integrity
  - McAfee Desktop Firewall 8.0
  - InfoExpress CyberGatekeeper Agent

- **Rule Settings**

  Eine ***Regel*** ist eine Anforderung, die ein Client erfüllen muss, damit die Hostprüfung eine Bestätigung an das IVE zurückgeben kann. Sie können fünf Typen von Regeln festlegen:

  - **Custom NHC integration**

    Geben Sie mit dieser Regel den Speicherort einer benutzerdefinierten DLL an, die anhand der Hostprüfungs-API geschrieben wird. Die Hostprüfung ruft die DLL auf, um benutzerdefinierte clientseitige Überprüfungen auszuführen. Wenn die DLL eine Bestätigung an die Hostprüfung zurückgibt, sieht das IVE die Regel als erfüllt an. Weitere Informationen über die Hostprüfungs-API finden Sie in der API-Dokumentation auf der NetScreen-Support-Site: http://support.netscreen.com.

  - **Port check**

    Verwenden Sie diese Regel, um von einem Clientcomputer das Öffnen bzw. Schließen bestimmter Ports für den Benutzerzugriff auf das IVE zu fordern.

  - **Process check**

    Verwenden Sie diese Regel, um vom Clientcomputer das Ausführen bzw. Unterdrücken eines bestimmten Prozesses für den Benutzerzugriff auf das IVE zu fordern.

  - **File check**

    Verwenden Sie diese Regel, um von einem Clientcomputer den Besitz bzw. das Fehlen einer bestimmten Datei für den Benutzerzugriff auf das IVE zu fordern.

  - **Registry settings check**

    Verwenden Sie diese Regel, um von einem Clientcomputer das Vorhandensein bestimmter Registrierungseinstellungen für den Benutzerzugriff auf das IVE zu fordern.

Sie können eine beliebige Anzahl von zu verwendenden Methoden und Regeln für die Hostprüfung auswählen, um zu überprüfen, ob ein Client über die erforderlichen Eigenschaften der Endpunktsicherheit verfügt. Diese

Regeln werden zu einer Richtlinie zusammengefasst, die von der Hostprüfung auf dem Client überprüft wird. Sie können dann den Zugriff auf das IVE und die Ressourcen durch Forderung einer Hostprüfung einschränken:

- **Richtlinie für Bereichsauthentifizierung**

  Wenn Administratoren versuchen, sich beim IVE anzumelden, wertet das IVE die Authentifizierungsrichtlinie des angegebenen Bereichs aus und ermittelt, ob die Hostprüfung zu den Anforderungen gehört, die vor der Authentifizierung erfüllt sein müssen. Sie können eine Richtlinie für die Bereichsauthentifizierung so konfigurieren, dass die Hostprüfung heruntergeladen wird, die Hostprüfung herunterladen und die für den Bereich festgelegten Hostprüfung-Richtlinien durchsetzen oder konfigurieren, dass keine Hostprüfung erforderlich ist. Der Benutzer muss sich von einem Computer anmelden, der den Hostprüfung-Anforderungen entspricht, die für den Bereich festgelegt wurden. Wenn dies nicht der Fall ist, leitet das IVE die Anmeldeinformationen des Benutzers nicht an den Authentifizierungsserver weiter, und der Benutzer kann nicht auf das IVE zugreifen.

- **Benutzerrolle**

  Wenn das IVE die Liste der zulässigen Rollen ermittelt, die einem Administrator oder Benutzer zugeordnet sind, wertet es die Einschränkungen der einzelnen Rollen aus. Dabei ermittelt es, ob das Gerät des Benutzers für die Rolle bestimmte Richtlinien für die Hostprüfung einhalten muss. Wenn dies der Fall ist und das Gerät des Benutzers die festgelegten Richtlinien für die Hostprüfung nicht einhält, ordnet das IVE den Benutzer dieser Rolle nicht zu.

- **Ressourcenrichtlinie**

  Wenn ein Benutzer eine Ressource anfordert, wertet das IVE die genauen Regeln der Ressourcenrichtlinie aus. Dabei ermittelt es, ob das Gerät des Benutzers für die betreffende Ressource bestimmte Richtlinien für die Hostprüfung einhalten muss. Wenn das Gerät des Benutzers den festgelegten Richtlinien für die Hostprüfung nicht entspricht, verweigert das IVE den Zugriff auf die betreffende Ressource.

Ausführung der Hostprüfung

Wenn Sie die Hostprüfung als Anforderung für eine Rolle oder Ressourcenrichtlinie festlegen möchten, muss der Agent bei der Anmeldung des Benutzers minimal installiert werden. Dies wird in der Authentifizierungsrichtlinie des Bereichs konfiguriert. Nach der Konfiguration lädt das IVE das ActiveX-Steuerelement auf das System des Benutzers herunter. Außerdem müssen Sie systemweite Richtlinien für die Hostprüfung definieren (Registerkarte **System > Configuration > Security > Hostprüfung**), aus denen Sie dann auswählen, wenn Sie eine Anforderung für die Hostprüfung für einen Bereich, eine Rolle oder eine Ressourcenrichtlinie konfigurieren.

Wenn ein Benutzer auf die Anmeldeseite des IVE zugreifen will, versucht das IVE, den Benutzer einer Rolle zuzuordnen. Oder der Benutzer fordert eine Ressource an, und der Hostprüfungs-Agents überprüft anhand der Methoden und Regeln, die Sie in der zugeordneten Richtlinie für die Hostprüfung festgelegt haben, ob der Client die Endpunktsicherheitsanforderungen erfüllt. Das IVE wartet bis zu 120 Sekunden darauf, dass die Hostprüfung eine Bestätigung oder Ablehnung zurückgibt. Nach Ablauf der Höchstdauer zeigt das IVE eine Fehlermeldung an, und der Benutzer wird auf die Anmeldeseite zurückgeleitet.

Wenn die Endpunktsicherheitsprüfung erfolgreich verläuft, zeigt das IVE dem authentifizierten Benutzer die Startseite an, weist ihn der entsprechenden Rolle zu oder führt die in der Ressourcenrichtlinie festgelegte Aktion durch. Schlägt die Prüfung fehl, wenn der Benutzer versucht, auf die Anmeldeseite des IVE zuzugreifen, zeigt das IVE eine Fehlermeldung mit der Information an, dass der Computer nicht der Richtlinie für die Endpunktsicherheit entspricht. Wenn die Prüfung bei der Auswertung einer Rollenzuordnungsregel durch das IVE fehlschlägt, ordnet das IVE den Benutzer nicht der entsprechenden Rolle zu. Schlägt die Prüfung fehl, wenn der Benutzer eine bestimmte Ressource anfordert, führt das IVE die Aktion nicht aus, die in der entsprechenden Ressourcenrichtlinie festgelegt ist.

Unabhängig von Erfolg oder Fehlschlagen verbleibt die Hostprüfung im Verzeichnis `C:\Programme\Neoteris\Host Checker` auf dem Client. Der Agent kann von Benutzern manuell deinstalliert werden, indem in diesem Verzeichnis die Datei `uninstall.exe` ausgeführt wird. Dieses Verzeichnis enthält außerdem eine Protokolldatei, die bei jedem Ausführen der Hostprüfung neu geschrieben wird.

Weitere Informationen zu den Optionen der Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 23.

Protokollierung und Überwachung – Übersicht

IVE-Protokolldateien sind auf dem IVE gespeicherte Textdateien, die zur Verfolgung von Systemereignissen dienen. Das IVE generiert drei Arten von Protokolldateien:

- **Events log** – Diese Protokolldatei enthält eine Reihe von Systemereignissen, wie z.B. Sitzungsabläufe (beispielsweise aufgrund von Leerlauf oder Überschreitung der Sitzungshöchstdauer), Systemfehler und -warnungen, Anforderungen zur Überprüfung der Serververbindung und Benachrichtigungen über einen Neustart des IVE-Dienstes. (Der IVE-Überwachungsprozess prüft in regelmäßigen Abständen den IVE-Server und startet ihn neu, falls das IVE nicht reagiert.)
- **User Access log** – Diese Protokolldatei enthält Informationen über Benutzerzugriffe auf das IVE, einschließlich der Anzahl gleichzeitig angemeldeter Benutzer jeweils nach Ablauf einer Stunde (Anmeldung zur vollen Stunde), Benutzeran- und -abmeldungen, Dateianforderungen durch Benutzer und Webanforderungen.
- **Administrator Access log** – Diese Protokolldatei enthält Administratorinformationen, einschließlich Änderungen des Administrators an den Benutzer-, System- und Netzwerkeinstellungen, beispielsweise Änderungen an der Sitzungshöchstdauer, an der Option zum Aktivieren bzw. Deaktivieren der URL-Navigation und an von Benutzern erstellten Lesezeichen sowie Geräte- und Serverinformationen. Außerdem wird bei jeder Anmeldung, Abmeldung oder Änderung von Lizenzen auf dem IVE durch einen Administrator ein Protokolleintrag erstellt.

Auf den Seiten **System > Log/Monitoring** können Sie angeben, welche Ereignisse protokolliert werden, die maximale Dateigröße für das Systemprotokoll festlegen und einstellen, ob Ereignisse zusätzlich zur lokalen Protokollierung auch auf dem Syslog-Server protokolliert werden sollen. Auf den Seiten **System > Log/Monitoring** können Sie die angegebene Anzahl von Ereignissen anzeigen, die Protokolldatei im Netzwerk speichern und den Inhalt der Protokolle löschen.

Wenn eins der Protokolle die konfigurierte maximale Dateigröße (standardmäßig 200 MB) erreicht, werden die aktuellen Daten in eine Sicherungsprotokolldatei verschoben. Dann wird eine neue, leere Datei für alle folgenden (neuen) Protokollmeldungen erstellt. Mithilfe des Protokollbetrachters kann der Administrator die letzten 5000 Protokollmeldungen (Anzeigebeschränkung des Betrachters) anzeigen. Wenn die aktuelle Protokolldatei weniger als 5000 Protokollmeldungen enthält, werden ältere Protokollmeldungen aus der Sicherungsprotokolldatei geöffnet, sodass insgesamt 5000 Protokollmeldungen angezeigt werden. Dabei werden die Protokollda-

teien wie eine einzige Datei angezeigt, obwohl sie aufgrund der konfigurierten maximalen Dateigröße getrennt gespeichert sind.

Wichtig: Wenn Sie die Protokollmeldungen speichern oder die FTP-Archivierungsfunktion auf der Seite **Maintenance > Archiving** verwenden möchten, wird die Sicherungsprotokolldatei an die aktuelle Protokolldatei angehängt, und beide werden anschließend als eine Protokolldatei heruntergeladen. Wenn die Protokolldateien nicht archiviert oder gespeichert werden, gehen die ältesten Protokollmeldungen (in der Sicherungsprotokolldatei gespeichert) beim nächsten Verschieben der aktuellen Protokolldatei in die Sicherungsprotokolldatei verloren.

Außerdem können Sie das IVE mit einem Netzwerkverwaltungstool wie HP OpenView als SNMP-Agent überwachen. Das IVE unterstützt SNMP v2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die NetScreen-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

Hinweis: Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt.

Weitere Informationen finden Sie unter:

Schweregrade der Protokolldatei 96
Benutzerdefinierte Filterung von Protokolldateien..... 97
Konfigurieren der Seite „Log Monitoring“ 187

Schweregrade der Protokolldatei

Ereignisse in den IVE-Protokolldateien für Ereignisse, Benutzerzugang und Administratorzugang werden anhand der folgenden Richtlinien hierarchisiert:

- **Critical (Sicherheitsstufe 10)** – Wenn das IVE Benutzer- und Administratoranforderungen nicht bedienen kann oder seine Funktionen für einen Großteil der Untersysteme verliert, wird ein kritisches Ereignis („Critical Event“) protokolliert.
- **Major (Sicherheitsstufe 8-9)** – Wenn das IVE seine Funktionen in mindestens einem Untersystem verliert, aber noch auf die Appliance für

andere Zugangsmechanismen zugreifen kann, wird ein größeres Ereignis („Major Event") protokolliert.

- **Minor (Sicherheitsstufe 5-7)** – Wenn das IVE einen Fehler findet, der keinem größeren Ausfall in einem Untersystem entspricht, wird ein kleineres Ereignis („Minor Event") protokolliert. Kleinere Ereignisse entsprechen üblicherweise einzelnen fehlgeschlagenen Anforderungen.
- **Info (Sicherheitsstufe 1-4)** – Wenn das IVE eine Benachrichtigungsmeldung anzeigt, ein Benutzer eine Anforderung vornimmt oder ein Administrator eine Änderung durchführt, wird ein Informationsereignis („Informational Event") protokolliert.

Benutzerdefinierte Filterung von Protokolldateien

Mit dem Central Manager-Paket können Sie die Daten in den Protokolldateien für Ereignisse, Benutzerzugriff und Administratorzugriff filtern und formatieren.

Wenn Sie Protokolldateien filtern, speichert das IVE nur die Meldungen, die in der Filterabfrage angegeben wurden. Sie können z.B. eine Abfrage erstellen, die nur Einträge für einen bestimmten IP-Adress-Bereich oder für Benutzer protokolliert, die in einem bestimmten Bereich angemeldet sind. Eine Abfrage wird mithilfe der IVE-Sprache für benutzerdefinierte Ausdrücke erstellt.

Wenn Sie Protokolldateien formatieren, ändert das IVE lediglich das Aussehen der Meldungen entsprechend Ihrer Angaben. Protokollformate wirken sich nicht auf die Auswahl von Daten aus, die das IVE speichert, sondern nur auf die Art, wie das IVE sie anzeigt. Das IVE umfasst Standard-, WELF- und W3C-Protokollformate, es steht Ihnen jedoch frei, benutzerdefinierte Formate zu erstellen. Benutzerdefinierte Formate können mithilfe der Protokollfelder erstellt werden.

Konfigurationsanweisungen finden Sie unter „Konfigurieren der Seite „Log Monitoring"" auf Seite 187.

Network Connect – Übersicht

Die Aktualisierungsoption Network Connect bietet Möglichkeiten zur Verwendung eines VPN ohne Client und stellt somit ein weiteres Verfahren für den Remotezugriff auf Unternehmensressourcen über das IVE bereit. Dieses Feature unterstützt alle Modi für den Internetzugang (einschließlich DFÜ-Verbindungen, Breitband und LAN-Szenarien) vom Clientcomputer aus und funktioniert bei Vorhandensein clientseitiger Proxys und Firewalls, die den SSL-Datenverkehr über Port 443 zulassen.

Wenn ein Benutzer Network Connect startet, wird der gesamte Datenverkehr zum und vom Client über den sicheren Network Connect-Tunnel übertragen. Die einzige Ausnahme besteht für Datenverkehr, der von anderen IVE-fähigen Features initiiert wird, z.B. Webbrowsing, Navigieren durch Dateien und Telnet/SSH. Wenn Sie für bestimmte Benutzer keine weiteren IVE-Funktionen aktivieren möchten, erstellen Sie eine Benutzerrolle, für die nur die Option Network Connect aktiviert ist. Achten Sie darauf, dass die Benutzer, die dieser Rolle zugeordnet sind, nicht noch weiteren Rollen zugeordnet sind, die weitere IVE-Funktionen aktivieren.

Beim Ausführen von Network Connect wird der Client wie ein Knoten im Remote-LAN (Unternehmens-LAN) behandelt und im lokalen LAN des Benutzers nicht mehr angezeigt. Das IVE wird als DNS-Gateway für den Client verwendet und verfügt über keine Informationen zum lokalen LAN des Benutzers. Benutzer können jedoch auf ihrem PC statische Routen festlegen, um bei bestehender Verbindung mit dem Remote-LAN weiterhin auf das lokale LAN zugreifen zu können. Da der gesamte PC-Datenverkehr über den Network Connect-Tunnel zu den internen Unternehmensressourcen übertragen wird, müssen Sie darauf achten, dass andere Hosts im lokalen Netzwerk des Benutzers keine Verbindung mit dem PC herstellen können, auf dem Network Connect ausgeführt wird.

Sie können sicherstellen, dass andere Hosts im lokalen LAN eines Remotebenutzers nicht auf die internen Unternehmensressourcen zugreifen können, indem Sie den Benutzerzugriff auf das lokale Subnetz verweigern. (Dies wird über die Registerkarte **Users > Roles >** *Rollenname* **> Network Connect** konfiguriert.) Wenn Sie keinen Zugriff auf das lokale Subnetz gewähren, beendet das IVE Network Connect-Sitzungen, die von Clients initiiert wurden, auf denen statische Routen festgelegt sind. Sie können festlegen, dass Clients vor dem Starten einer Remotezugriffssitzung auf Netzwerkebene Lösungen für die Endpunktsicherheit ausführen müssen, z.B. eine persönliche Firewall. Mit der Hostprüfung, die auf Hosts, die mit dem IVE eine Verbindung herstellen, Endpunktsicherheitsprüfungen durchführt, kann sichergestellt werden, dass die Clients Endpunktsicherheitssoftware verwenden. Weitere Informationen finden Sie unter „Hostprüfung – Übersicht“ auf Seite 91.

Informationen über die Konfiguration von Ressourcenrichtlinien für Network Connect finden Sie unter „Konfigurieren der Seite „Network Connect"" auf Seite 369.

Ausführen von Network Connect

Der Network Connect-Agent (NC) wird wie folgt ausgeführt:

1. Ein Benutzer meldet sich am IVE an und klickt auf der IVE-Startseite auf die Verknüpfung für **Network Connect**.
2. Anschließend wird vom IVE ein ActiveX-Steuerelement auf den Clientcomputer heruntergeladen, das die folgenden Aktionen ausführt:
   1. Das IVE ermittelt, ob Network Connect installiert ist. Wenn dies nicht der Fall ist, installiert das IVE die erforderliche Software in einem einmaligen Setup.
   2. Der Dienst Network Connect sendet eine Anforderung an das IVE, um die Verbindung mit einer IP-Adresse aus dem zuvor bereitgestellten IP-Pool zu initialisieren.
   3. Das System Tray-Symbol für Network Connect wird auf der Taskleiste angezeigt.
3. Das IVE reserviert zwei IP-Adressen aus dem konfigurieren Pool und weist folgenden Elementen eine eindeutige IP zu:
   - Dem NC-Dienst, der auf dem Client ausgeführt wird.
   - Dem NC-Prozess, der im IVE ausgeführt wird.
4. Der clientseitige Network Connect-Dienst verwendet die zugewiesenen IP-Adressen für die Kommunikation mit dem im IVE ausgeführten Network Connect-Prozess.
5. Der serverseitige Network Connect-Prozess verwendet die zugewiesene IP-Adresse für die Kommunikation mit Unternehmensressourcen.

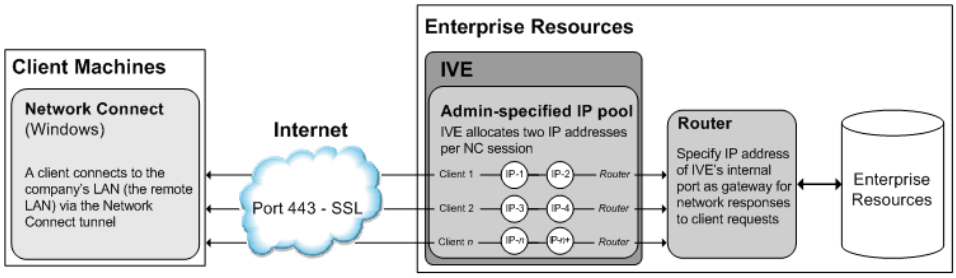


Abbildung 6: Client/Server-Kommunication mit Network Connect

Der clientseitige Network Connect-Dienst kommuniziert mit dem im IVE ausgeführten serverseitigen Network Connect-Prozess. Dieser Prozess leitet Clientanforderungen an Unternehmensressourcen weiter.

Durchgangsproxy – Übersicht

Mithilfe der Durchgangsproxy-Funktion können Sie Webanwendungen angeben, für die das IVE eine minimale Vermittlung durchführt. Anders als die herkömmliche Antwortproxyfunktion, bei der ebenfalls nur selektive Teile einer Serverantwort neu geschrieben werden, jedoch sowohl Netzwerkänderungen als auch komplexe Konfigurationen vorgenommen werden müssen, müssen Sie für diese Funktion lediglich Anwendungsserver und die Methode angeben, mit der das IVE Clientanforderungen an diese Anwendungsserver empfängt:

- **Via an IVE port**

  Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Port an, an dem das IVE Clientanforderungen an den Anwendungsserver abfragen soll. Wenn das IVE eine Clientanforderung für den Anwendungsserver empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport weiter. Wenn Sie diese Option auswählen, müssen Sie bei Ihrer Firmenfirewall den Datenverkehr für den angegebenen IVE-Port freigeben.

- **Via external DNS resolution**

  Wenn Sie eine Anwendung zur Vermittlung für den Durchgangsproxy angeben, geben Sie einen Alias für den Hostnamen des Anwendungsservers ein. Für diesen Alias müssen Sie einen Eintrag im externen DNS vornehmen, der für das IVE aufgelöst wird. Wenn das IVE eine Clientanforderung für den Alias empfängt, leitet es die Anforderung an den für den Anwendungsserver angegebenen Port weiter.

  Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für den Zugriff auf das IVE eingerichtet wurden. Wenn Sie diese Option verwenden, ist es empfehlenswert, dass jeder Hostnamenalias dieselbe Domänenteilzeichenfolge enthält wie der IVE-Hostname und dass Sie ein Serverzertifikat mit Platzhalter in folgendem Format in das IVE hochladen: `*.domaene.de`.

  Wenn das IVE beispielsweise `iveserver.firmenname.de` lautet, muss der Hostnamenalias im Format `anwserver.firmenname.de` und mit Platzhalter im Format `*.firmenname.de` angegeben werden. Wenn Sie kein Zertifikat mit Platzhalter verwenden, stellt der Browser eines Clients eine Warnung zu einer Zertifikatsnamenüberprüfung aus, wenn ein Benutzer zu einem Anwendungsserver wechselt, da der Hostnamenalias des Anwendungsservers nicht mit dem Zertifikatsdomänennamen übereinstimmt. Dies hindert einen Benutzer jedoch nicht daran, auf den Anwendungsserver zuzugreifen.

Beispiele

Wenn das IVE den Namen `iveserver.firmenname.de` hat und Sie über einen Oracle-Server bei `oracle.firmennetzwerk.net:8000` verfügen, könnten Sie diese Anwendungsparameter bei der Angabe eines IVE-Ports angeben:

```
Server: oracle.firmennetzwerk.net
Port: 8000
IVE Port: 11000
```

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an `iveserver.firmenname.de:11000` gesendet wurde, leitet es den Verkehr an `oracle.firmennetzwerk.net:8000` weiter.

Wenn Sie einen Hostnamenalias angeben möchten, können Sie die Anwendung mit folgenden Parametern konfigurieren:

```
Server: oracle.firmennetzwerk.net
Port: 8000
IVE Alias: oracle.firmenname.de
```

Wenn das IVE Datenverkehr vom Oracle-Client empfängt, der an `oracle.firmenname.de` gesendet wurde, leitet es den Datenverkehr an `oracle.firmennetzwerk.net:8000` weiter.

Wenn Sie Clientanforderungen an das IVE anhand des Hostnamenalias weiterleiten, müssen Sie das IVE außerdem dem externen DNS-Server hinzufügen. Diese Option bietet sich an, wenn in Ihrem Unternehmen restriktive Richtlinien für das Öffnen von Firewallports für interne Server oder Server in der DMZ gelten.

Ebenso wie das eigentliche Vermittlungsmodul bietet die Durchgangsproxy-Option eine höhere Sicherheit als Secure Application Manager, da das IVE dem Client bei Aktivierung für eine Anwendung ermöglicht, nur Layer-7-Verkehr an feste Anwendungsports an das Firmennetzwerk zu senden. Wenn diese Option aktiviert ist, kann das IVE Anwendungen mit Komponenten unterstützen, die nicht mit dem Modul für die Inhaltsvermittlung kompatibel sind, beispielsweise Java-Applets in Anwendungen der Oracle E-Business Suite oder Applets, die auf einer nicht unterstützten Java Virtual Machine ausgeführt werden.

Hinweis: Die Durchgangsproxy-Option kann nur für Anwendungen verwendet werden, die feste Ports abfragen und bei denen der Client keine direkten Socketverbindungen herstellt.

Informationen zum Angeben von Anwendungen, für die das IVE eine minimale Vermittlung durchführt, finden Sie unter „Schreiben einer Ressourcenrichtlinie für Durchgangsproxys“ auf Seite 341.

Remote SSO – Übersicht

Mithilfe der Funktion Remote-SSO (Single Sign-On, Einzelanmeldung) können Sie einen Anmeldeseiten-URL einer Anwendung angeben, an die das IVE die Anmeldeinformationen eines Benutzers senden soll. Dadurch wird vermieden, dass Benutzer ihre Anmeldeinformationen für den Zugriff auf verschiedene Back-End-Anwendungen mehrmals angeben müssen. Sie können außerdem zusätzliche Formularwerte und benutzerdefinierte Header (einschließlich Cookies) angeben, die an das Anmeldeformular einer Anwendung gesendet werden.

Für die Remote-SSO-Konfiguration müssen Webressourcenrichtlinien angegeben werden:

- **Form-POST-Richtlinie**

  Diese Art von Remote-SSO-Richtlinie gibt den Anmeldeseiten-URL einer Anwendung an, an die IVE-Daten und die zu veröffentlichenden Daten gesendet werden sollen. Diese Daten können den IVE-Benutzernamen und das IVE-Benutzerkennwort sowie die Systemdaten enthalten, die in Systemvariablen gespeichert sind („Systemvariablen und Beispiele“ auf Seite 442). Sie können außerdem angeben, ob Benutzer diese Informationen ändern dürfen.

- **Header/Cookies-Richtlinie**

  Diese Art von Remote-SSO-Richtlinie gibt Ressourcen wie benutzerdefinierte Anwendungen an, an die benutzerdefinierte Header und Cookies gesendet werden können.

Wenn sich die Anmeldeinformationen eines Benutzers von denen unterscheiden, die die Back-End-Anwendung benötigt, kann der Benutzer auch folgendermaßen auf die Anwendung zugreifen:

- **Manuelle Anmeldung**

  Der Benutzer kann schnell auf die Back-End-Anwendung zugreifen, indem er auf der Anmeldeseite der Anwendung seine Anmeldeinformationen manuell eingibt. Der Benutzer kann seine Anmeldeinformationen und sonstige erforderliche Daten auch entsprechend der folgenden Beschreibung über die Seite **Advanced Preferences** dauerhaft im IVE speichern. Dieser Vorgang ist jedoch optional.

- **Angeben der erforderlichen Anmeldeinformationen auf dem IVE**

  Der Benutzer muss für das IVE die Anmeldeinformationen für die Anwendung fehlerfrei angeben. Die Informationen werden auf der Seite **Advanced Preferences** festgelegt. Nach dem Festlegen muss sich der Benutzer abmelden und erneut anmelden, um seine Anmeldeinformationen für das IVE zu speichern. Wenn der Benutzer das nächste Mal auf das

Remote-SSO-Lesezeichen klickt, um sich bei der Anwendung anzumelden, sendet das IVE die aktualisierten Anmeldeinformationen.

Hinweis: Übergeben Sie mithilfe der Remote-SSO-Funktion Daten an Anwendungen, in deren HTML-Formularen statische POST-Aktionen enthalten sind. Es empfiehlt sich nicht, Remote-SSO mit Anwendungen zu verwenden, bei denen sich regelmäßig ändernde URL POST-Aktionen zur Anwendung kommen, ein Ablauf nach einer bestimmten Zeit auftritt oder POST-Aktionen ablaufen, die zum Zeitpunkt der Erstellung des Formulars generiert wurden.

Secure Application Manager – Übersicht

Die Aktualisierungsoption Secure Application Manager ermöglicht sicheren Remotezugriff von Clientanwendungen auf Unternehmensserver auf Anwendungsebene. Sie können zwei Versionen von Secure Application Manager bereitstellen.

- **Windows-Version (W-SAM)**

  Die Windows-Version von Secure Application Manager ist eine Windows-32-Lösung für die sichere, transparente Umleitung ausgehender TCP-Verbindungen über ein IVE-Gerät für jeweils eine Anwendung oder einen Host. Die Software wird von einem im IVE gehosteten ActiveX-Steuerelement heruntergeladen und gestartet. Weitere Informationen finden Sie unter „Windows Secure Application Manager (W-SAM) – Übersicht" auf Seite 109.

- **Java-Version (J-SAM)**

  Die Java-Version des Secure Application Manager bietet Unterstützung für TCP-Client/Server-Anwendungen mit statischen Ports, einschließlich erweiterter Unterstützung von Microsoft MAPI, Lotus Notes und Citrix NFuse. J-SAM unterstützt zudem NetBIOS, wodurch Benutzer bestimmten geschützten Ressourcen Laufwerke zuordnen können. J-SAM funktioniert fehlerfrei in einer Vielzahl von Netzwerkkonfigurationen, wobei TCP-Client/Server-Anwendungen mit dynamischen Ports, vom Server initiierte Verbindungen oder UDP-Datenverkehr jedoch nicht unterstützt werden. J-SAM reserviert bei der Ausführung 20 bis 30 MB RAM (die genaue Speichermenge hängt vom verwendeten JVM ab) und behält, falls die Zwischenspeicherung aktiviert ist, auf dem Clientcomputer eine JAR-Datei bei. Weitere Informationen finden Sie unter „Java Secure Application Manager (J-SAM) – Übersicht" auf Seite 111.

Hinweis: Gegenwärtig wird auf Windows-, Linux- oder Macintosh-Plattformen Sun JVM, Version 1.4.1 oder höher unterstützt. Die MS JVM, die auf Sun JRE, Version 1.1 beruht, wird unter Windows ebenfalls unterstützt.

Windows Secure Application Manager (W-SAM) – Übersicht

Die Windows-Version von Secure Application Manager (W-SAM) ist ein Dienst, der anhand des LSP-Verfahrens (Layered Service Provider) Datenverkehr von Clientanwendungen sichert, die auf einem PC ausgeführt werden. Die LSP-Dienstkomponenten werden auf einem Client-PC anhand eines ActiveX-Steuerelements installiert, das heruntergeladen wird, wenn ein Benutzer Secure Application Manager über die IVE-Startseite startet. Nach der Installation fängt Secure Application Manager Folgendes ab:

- TCP-Verbindungsaufrufe von im IVE konfigurierten Anwendungen
- DNS-Abfragen für im IVE konfigurierten Zielhostnamen

Wenn ein Benutzer Secure Application Manager startet[1], wird ein Statusfenster als Prozess im System Tray ausgeführt. Benutzer können auf dieses Symbol doppelklicken, um den aktuellen Sitzungsstatus und eine Liste von Anwendungen und Hosts anzuzeigen, die für die Vermittlung über Secure Application Manager angegeben sind.

Client/Server-Kommunikation mithilfe von W-SAM

Die folgende Abbildung verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE.

1. Zum Starten von Windows Secure Application Manager klicken Benutzer auf die IVE-Menüoption für Secure Application Manager. Das IVE lädt das ActiveX-Steuerelement auf den Clientcomputer herunter. Dieses Steuerelement konfiguriert den Clientcomputer zum Ausführen von clientseitigen Diensten (LSP), um den Anwendungsverkehr zu sichern. Das Statusfenstersymbol für den Secure Application Manager wird im System Tray angezeigt.
2. Der Benutzer startet eine vom Administrator festgelegte Anwendung oder initiiert einen Prozess, der Daten von einem angegebenen Host anfordert. Wenn die Clientanwendung oder der Prozess versucht, eine Verbindung mit der Ressource herzustellen, fängt Secure Application Manager die Anforderung ab.
3. Secure Application Manager leitet den Hostnamen über SSL an das IVE weiter. Das IVE löst den Hostnamen auf und gibt die IP-Adresse des Zielhosts an Secure Application Manager zurück.
4. Secure Application Manager konfiguriert automatisch einen Kanal für die Portumleitung. Dazu wird die bereits vorkonfigurierte IP-Adresse `localhost` verwendet.

1. Sie können Secure Application Manager so konfigurieren, dass er bei der Anmeldung eines Benutzers automatisch gestartet wird. Benutzer können diese Einstellung über das Menü IVE **System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Startseitenmenü geklickt wird.

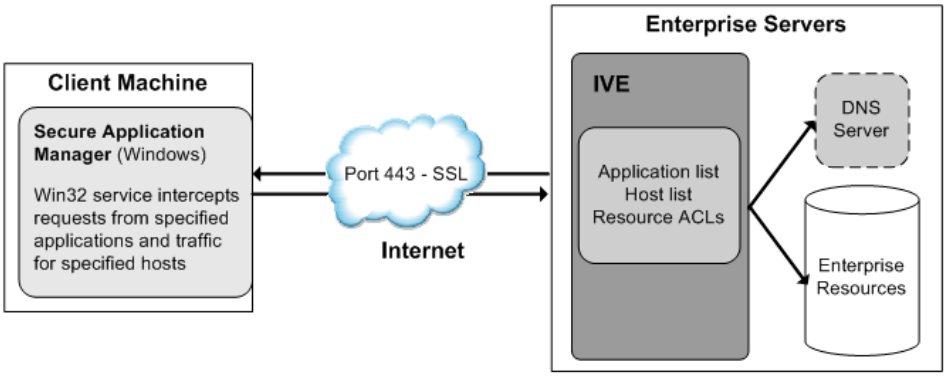


Abbildung 7: Windows Secure Application Manager

Java Secure Application Manager (J-SAM) – Übersicht

Die Java-Version von Secure Application Manager (J-SAM) bietet sichere Portweiterleitung für Anwendungen, die auf einem Remotecomputer ausgeführt werden. Das IVE weist jedem Anwendungsserver, den Sie für einen bestimmten Port festlegen, eine eindeutige IP-Loopback-Adresse zu. Wenn Sie beispielsweise für einen einzigen Port folgendes festlegen:

`app1.eigenefirma.de, app2.eigenefirma.de, app3.eigenefirma.de, ...`

weist das IVE jeder Anwendung eine eindeutige IP-Loopback-Adresse zu:

`127.0.1.10, 127.0.1.11, 127.0.1.12, ...`

Wenn ein Benutzer J-SAM herunterlädt, überwacht J-SAM die vom IVE zugewiesenen Loopback-Adressen (am entsprechenden, für den Anwendungsserver festgelegten Clientport) auf Clientanforderungen an die Netzwerkanwendungsserver. J-SAM kapselt die Anforderungsdaten und leitet die verschlüsselten Daten als SSL-Verkehr an das IVE weiter. Das IVE entkapselt die Daten und leitet sie an den festgelegten Serverport auf dem Anwendungsserver im Netzwerk weiter. Der Anwendungsserver gibt seine Antwort an das IVE weiter, das die Daten entkapselt und sie an J-SAM weiterleitet. J-SAM entkapselt dann die Antwort des Servers und leitet die Daten an die Clientanwendung weiter. Für die auf dem lokalen Computer ausgeführte Clientanwendung fungiert J-SAM als Anwendungsserver. Für den Anwendungsserver in Ihrem Netzwerk übernimmt das IVE die Rolle der Clientanwendung.

J-SAM stellt außerdem Folgendes bereit:

- Erweiterte Unterstützung für MS Exchange 116
- Erweiterte Unterstützung für Lotus Notes..... 119
- Erweiterte Unterstützung für Citrix NFuse 120

Client/Server-Kommunikation mithilfe von J-SAM

Die folgende Abbildung verdeutlicht die Interaktion zwischen einer Clientanwendung und dem Server über das IVE. In dieser Abbildung wird vorausgesetzt, dass der Benutzer in der Clientanwendung eine IP-Adresse für `localhost` als Server festlegt. Wenn Sie das IVE für die Verwendung der automatischen Hostzuordnung (für PC-Benutzer) konfigurieren, beachten Sie „Client/Server-Kommunikation mithilfe von J-SAM“ auf Seite 112.

1. Der Benutzer startet eine auf der Seite **Client Applications** des IVE aufgeführte Clientanwendung. Die Anwendung löst den Remoteserver in `localhost` auf.
2. Die Clientanwendung nimmt Verbindung mit dem auf dem Computer des Benutzers ausgeführten J-SAM auf und beginnt mit dem Senden von Anforderungen.
3. J-SAM kapselt alle Clientanforderungen und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und leitet sie zum festgelegten Anwendungsserver weiter.
5. Der Anwendungsserver antwortet mit Daten an den IVE-Server.
6. Das IVE kapselt die Antwort und leitet die Antwort vom Anwendungsserver über SSL an J-SAM weiter.
7. J-SAM entkapselt die Anwendungsserverdaten und leitet sie an die Clientanwendung weiter.

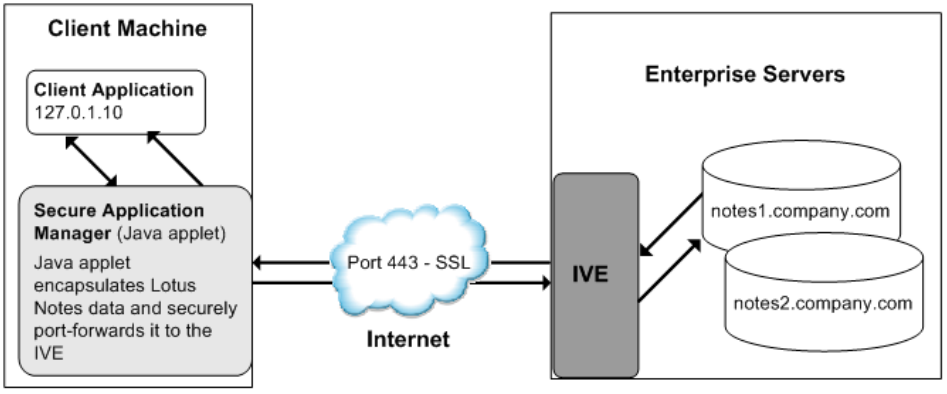


Abbildung 8: Java Secure Application Manager
In dieser Abbildung wird vorausgesetzt, dass der Benutzer in der Clientanwendung eine IP-Adresse für `localhost` als Server festlegt.

Hostnamenauflösung in `localhost`

Damit diese Lösung ordnungsgemäß funktioniert, muss eine Clientanwendung auf dem Benutzercomputer den Anwendungsserver in den Client (`localhost`) auflösen, sodass J-SAM die für den Anwendungsserver bestimmten Daten erfassen und über das IVE sicher über Ports leiten kann. J-SAM kann eine automatische Hostzuordnung ausführen, wobei die Datei `hosts` auf dem Client bearbeitet wird, um Anwendungsserver zum `localhost` zuzuordnen. Damit J-SAM die Datei `hosts` eines Benutzers bearbeiten kann, muss der Benutzer über die entsprechenden Rechte auf dem Clientcomputer verfügen:

- **Windows 2000-Benutzer** können einer beliebigen Benutzergruppe angehören. Für die Exchange MAPI-Unterstützung müssen Benutzer auf dem betreffenden Computer jedoch mindestens über Hauptbenutzerberechtigungen verfügen.
- **Windows XP-Benutzer** müssen über Administratorberechtigungen auf ihren Computern verfügen.
- **Benutzer von Linux (RedHat)** müssen den Browser, in dem J-SAM gestartet wird, als `root` aufrufen.
- **Macintosh-Benutzer** müssen das Administratorkennwort eingeben, wenn Sie von J-SAM eine entsprechende Aufforderung erhalten.

Wenn Benutzer nicht über die entsprechenden Berechtigungen auf ihren Computern verfügen, kann J-SAM die Datei `hosts` nicht automatisch verarbeiten, und die Hostnamenauflösung in `localhost` findet nicht statt. Benutzer ohne die entsprechenden Berechtigungen haben die folgenden Alternativen:

- Sie können ihren externen DNS-Server zum Auflösen von Anwendungsservern in `localhost` konfigurieren. Wenn Sie Ihren externen DNS-Server so konfigurieren, dass er eine `localhost`-Adresse anstelle des Hostnamens des Anwendungsservers verwendet, müssen Remotebenutzer die Reihenfolge, in der ihr Computer nach DNS-Servern sucht, so konfigurieren, dass mit der Firmen-DNS begonnen wird.
- Sie definieren weniger strikte Berechtigungen für das Verzeichnis `etc` und die Datei `etc\hosts`, um J-SAM das Ausführen der notwendigen Änderungen zu ermöglichen.
- Benutzer konfigurieren eines Clientanwendung für die Verwendung der `localhost`-Adresse, die durch das IVE zugewiesen wurde, indem sie normalerweise in der Clientanwendung den Hostnamen des Anwendungsservers angeben. Weitere Informationen finden Sie unter „Ermitteln der vom IVE zugewiesenen Loopback-Adresse“ auf Seite 115.

Zugriff auf privilegierte Ports für Benutzer von Linux und Macintosh

Linux-Benutzer haben keinen Zugriff auf Ports unter 1024, wenn sie auf Ihrem Computer nicht als `root` angemeldet sind. Macintosh-Benutzer haben keinen Zugriff auf Ports unter 1024, es sei denn, sie geben bei einer entsprechenden Aufforderung durch J-SAM das Administratorkennwort ein. So unterstützen Sie Anwendungen, die über privilegierte Ports (Ports unter 1024) ausgeführt werden, beispielsweise eine Telnet-Anwendung:

- Benutzer können den Browser, in dem J-SAM gestartet wird, als `root` starten.
- Sie oder der Benutzer können eine Client-Portnummer ab Port 1024 angeben, wenn Sie die Anwendung der Liste **Client Applications** hinzufügen.

  Wenn beispielsweise für eine Telnet-Anwendung als Clientport 2041 und als Serverport 23 angegeben ist, wird folgender Befehl zum Ausführen der Anwendung verwendet:

  `telnet` *`loopbackIP`* `2041`

  Dabei steht *`loopbackIP`* für die IP-Loopback-Adresse, die dem Anwendungsserver vom IVE zugewiesen wurde. J-SAM überwacht Port 2041 auf Datenverkehr von der Telnet-Anwendung und leitet diesen an das IVE weiter. Das IVE leitet den Datenverkehr dann an Port 23 auf dem Zielserver

weiter. Weitere Informationen über die Ermittlung der vom IVE zugewiesenen Loopback-Adresse finden Sie unter „Ermitteln der vom IVE zugewiesenen Loopback-Adresse“ auf Seite 115.

Ermitteln der vom IVE zugewiesenen Loopback-Adresse

Benutzer können den Firmen-DNS-Server für Anwendungen nicht ändern, der für die Portweiterleitung hinzugefügt werden. Wenn Sie Benutzern das Angeben von Anwendungen ermöglichen, für die J-SAM als Proxy fungieren soll, müssen diese eine Clientanwendung konfigurieren, um die Adresse des `localhost` verwenden zu können, die vom IVE zugewiesen wurde, in dem sie normalerweise den Hostnamen des Servers eingeben.
Im Fensterausschnitt **Details** des J-SAM-Browserfensters wird neben dem vom Benutzer angegebenen Port die IP-Loopback-Adresse angezeigt, die vom IVE zugewiesen wird. Um zu bestimmen, welche IP-Adresse das IVE einer auf der Seite **Client Applications** IVE angegebenen Anwendung zuweist, muss ein Benutzer nach dem Hinzufügen der Anwendung Secure Application Manager neu starten. Die der Anwendung zugewiesene Loopback-Adresse wird im Fensterausschnitt **Details** des Secure Application Manager-Browserfensters angezeigt:

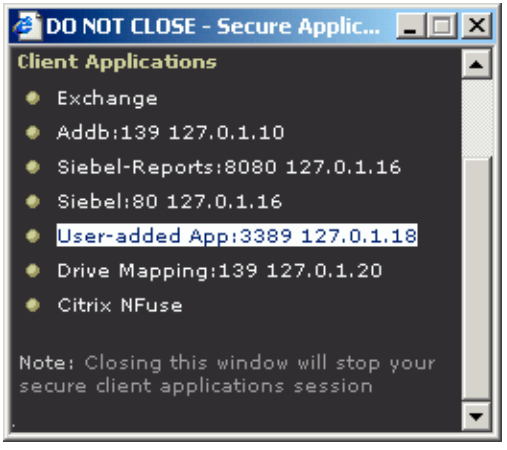


Abbildung 9: Fensterausschnitt „Details“ des Secure Application Manager (J-SAM)

In der Clientanwendung muss der Benutzer die vom IVE zugewiesene Loopback-Adresse als Anwendungsserver eingeben. Wenn ein Benutzer beispielsweise auf einen Telnet-Server hinter Ihrer Firmenfirewall zugreifen möchte, muss er die folgenden Schritte ausführen:

1. Klicken Sie auf der IVE-Seite **Client Applications** auf **Add Application**.

2. Geben Sie auf der Seite **Add Application** Folgendes an:
   - Im Feld **Remote Server** den vollständig qualifizierten Domänennamen oder die IP-Adresse des Servers, beispielsweise terminalserver.netscreen.com.
   - Im Feld **Client Port** den Port, der von J-SAM auf Datenverkehr von Clients zum Server überwacht werden soll, beispielsweise 3389.
   - Im Feld **Server Port** den Port, den der Remoteserver auf Datenverkehr von der Clientanwendung (J-SAM) überwachen soll, beispielsweise 3389.
3. Klicken Sie auf **Add**, um die Informationen zu speichern.
4. Schließen Sie das **Secure Application Manager**-Browserfenster.
5. Klicken Sie auf der Seite IVE **Client Applications** auf **Start Session**, um Secure Application Manager neu zu starten.
6. Klicken Sie im **Secure Application Manager**-Browserfenster auf **Details**.
7. Sehen Sie auf der Registerkarte **Details** nach, welche Loopback-Adresse das IVE dem Remoteserver zugewiesen hat, beispielsweise 127.0.1.18.
8. Geben Sie in der Clientanwendung (beispielsweise Remote Desktop Connection) die Loopback-Adresse im Konfigurationsfeld für den Server an. Dieses Feld wird in den einzelnen Anwendungen an unterschiedlicher Stelle angezeigt. Benutzer können diese Angaben über einen Setup-Assistenten oder ein sonstiges Dialogfeld für die Konfiguration eingeben.

Erweiterte Unterstützung für MS Exchange

Remotebenutzer können den Microsoft Outlook-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Outlook-Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Outlook-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie z.B. ein VPN, erforderlich. Diese Funktion erfordert die Installation der Microsoft JVM auf dem Client-PC und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt. Diese Funktion ist auch kompatibel mit PCs unter Windows 98 (mit Internet Explorer 5.5) oder Windows XP (mit Internet Explorer 6.0).

Damit diese Funktion von Remotebenutzern verwendet werden kann, muss der im Outlook-Client eingebettete Name der Exchange-Server von den Netzwerkeinstellungen des Benutzer-PCs zum lokalen PC (127.0.0.1, die Standard-IP-Adresse des `localhost`) aufgelöst werden, um einen sicheren Datenverkehr für den Outlook-Client zu gewährleisten. Wir empfehlen, das IVE für die automatische Auflösung von Exchange Server-Hostnamen in `localhost` zu konfigurieren, indem Sie die Datei `hosts` vorübergehend durch die Option für die automatische Hostzuordnung auf einem Clientcomputer aktualisieren.

Client/Server-Kommunikation mithilfe von J-SAM

Die folgende Abbildung beschreibt die Interaktionen zwischen dem Outlook-Client und einem Exchange-Server über das IVE. Diese Abbildung setzt voraus, dass das IVE für die automatische Hostzuordnung konfiguriert ist.

1. Der Benutzer startet den MS Outlook-Client. Outlook versucht, eine Verbindung mit dem Exchange Server `exchange1.ihrefirma.com` herzustellen. Das IVE löst den Hostnamen des Exchange-Servers durch temporäre Änderungen an der Datei `hosts` zu 127.0.0.1 (`localhost`) auf.
2. Outlook stellt eine Verbindung mit Secure Application Manager her, der auf dem PC des Benutzers ausgeführt wird, und beginnt dann, Anforderungen für E-Mail zu senden.
3. Secure Application Manager kapselt alle Anforderungen und leitet diese über SSL vom Outlook-Client an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und sucht in der MAPI-Anforderung nach dem Exchange-Zielserver. Die Anforderung wird dann an den Zielserver weitergeleitet.
5. Jede Anforderung im MAPI-Protokoll codiert den Zielserver für die Anforderung. Wenn von Secure Application Managerstammende MAPI-Anforderungen eingehen, werden sie vom IVE-Server überprüft und jeweils zum entsprechenden Zielserver weiterverteilt. Dieser Prozess wird auch bei Vorhandensein mehrerer Exchange-Server unbemerkt ausgeführt.
6. Der Exchange-Server antwortet dem IVE mit E-Mail-Daten.
7. Das IVE kapselt die Antwort und leitet sie vom Exchange-Server über SSL an Secure Application Manager weiter.
8. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale MAPI-Antwort vom Exchange-Server an dem Outlook-Client weiter.

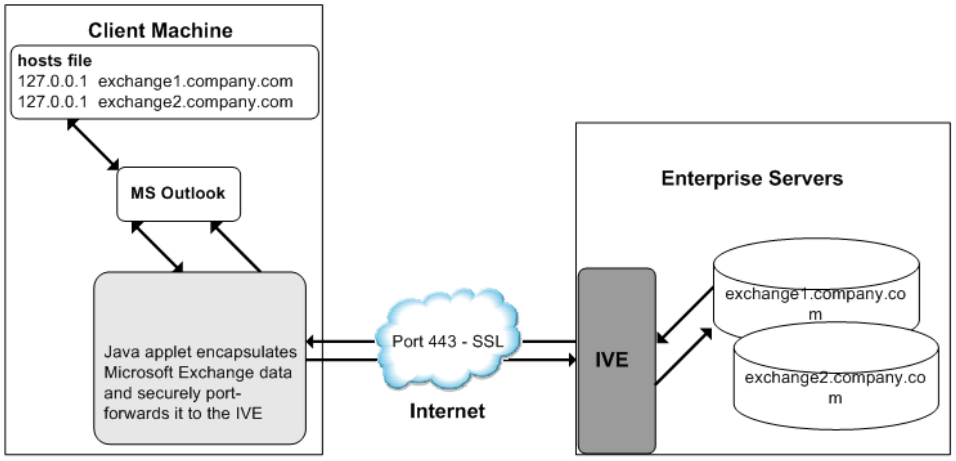


Abbildung 10: Java Secure Application Manager und erweiterte MS Exchange-Unterstützung

In dieser Abbildung wird das für die automatische Hostzuordnung für den MS Outlook-Client konfigurierte IVE dargestellt.

Aktualisierungen der Windows-Registrierung

Beim Start von Secure Application Manager wird die Windows-Registrierungseinstellung `Rpc_Binding_Order` des Benutzers aktualisiert. Diese Einstellung wird der Registrierung hinzugefügt, wenn der Outlook-Client installiert wird, und bestimmt die Protokollsequenz, die der Client zum Kommunizieren mit dem Exchange-Server verwendet.

Der ursprüngliche Wert dieser Einstellung ist:
ncalrpc,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp

Nach dem erstmaligen Verwenden von Secure Application Manager ist der Wert:
ncalrpc,ncacn_http,ncacn_ip_tcp,ncacn_spx,ncacn_np,
netbios,ncacn_vns_spp

Die Änderung an Rpc_Binding_Order betrifft nur die Ausführung von Secure Application Manager und hat keine anderen Auswirkungen auf dem PC des Benutzers.

Wichtig: Zum Verwenden des Outlook-Client über die Java-Version von Secure Application Manager müssen Benutzer von Windows-PCs über Administratorberechtigungen verfügen.

Erweiterte Unterstützung für Lotus Notes

Remotebenutzer können den Lotus Notes-Client auf ihren PCs zum Zugreifen auf E-Mail, ihre Kalender und andere Funktionen über das IVE verwenden. Dafür müssen keine Änderungen am Lotus Notes-Client vorgenommen werden, und es ist keine Verbindung auf Netzwerkebene, wie beispielsweise ein VPN, erforderlich. Diese Funktion benötigt die Microsoft oder Sun JVM und wird auf PCs unter Windows 2000 (mit Internet Explorer 5.5 oder 6.0) unterstützt.

Client/Server-Kommunikation mithilfe von J-SAM

Damit Remotebenutzer diese Funktion verwenden können, müssen sie den Lotus Notes-Client zum Verwenden von „`localhost`" als Einstellung für den Remotestandort konfigurieren. Secure Application Manager nimmt dann vom Lotus Notes-Client angeforderte Verbindungen auf. Die folgende Abbildung beschreibt die Interaktionen zwischen dem Lotus Notes-Client und einem Lotus Notes-Server über das IVE.

1. Der Benutzer startet den Lotus Notes-Client mit der Home Location-Einstellung. Der Client ermittelt die Proxyeinstellung, d.h. den `localhost`, den PC des Benutzers, für seine Home Location-Einstellung.
2. Der Lotus Notes-Client stellt eine Verbindung mit Secure Application Manager her, und beginnt damit, Anforderungen für E-Mail zu senden.
3. Secure Application Manager kapselt Anforderungen vom Lotus Notes-Client und leitet diese über SSL an das IVE weiter.
4. Das IVE entkapselt die Clientdaten und ermittelt den Lotus Notes-Zielserver in der Lotus Notes-Anforderung. Die Anforderung wird dann an den Zielserver weitergeleitet.

   Jede Anforderung im Lotus Notes-Protokoll codiert den Zielserver für die Anforderung. Wenn Lotus Notes-Anforderungen vom Anwendungsproxy eingehen, ruft der IVE-Server die Zielserverinformationen von den Anforderungen ab und verteilt die Anforderungen an den entsprechenden Zielserver weiter. Deshalb wird diese Funktion auch dann transparent ausgeführt, wenn von einem einzigen Benutzer auf mehrere Lotus Notes-Server zugegriffen wird.
5. Der Lotus Notes-Server antwortet dem IVE mit E-Mail-Daten.
6. Das IVE kapselt die Antwort vom Lotus Notes-Server und leitet diese über SSL an Secure Application Manager weiter.
7. Secure Application Manager entkapselt die vom IVE gesendeten Informationen und leitet die normale Antwort vom Lotus Notes-Server an den Lotus Notes-Client weiter.

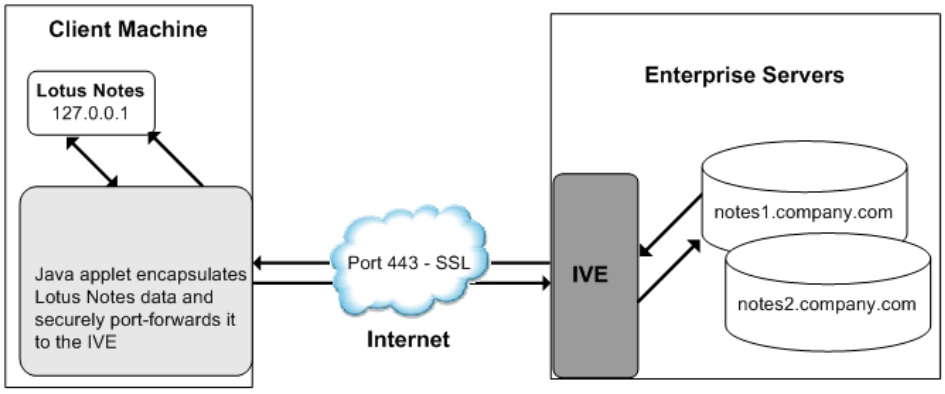


Abbildung 11: Java Secure Application Manager und erweiterte Lotus Notes-Unterstützung

In dieser Abbildung wird der Remotestandortwert des Lotus Notes-Clients dargestellt, der auf dem `localhost` konfiguriert wird.

Erweiterte Unterstützung für Citrix NFuse

Wenn ein Benutzer auf einem NFuse-Server eine Anwendung auswählt, sendet der NFuse-Server eine ICA-Datei an den Client. Wenn das IVE die ICA-Datei überschreibt, ersetzt es Hostnamen und IP-Adressen durch vorher bereitgestellte IP-Adressen des `localhost`. Der ICA-Client sendet dann Anwendungsanforderungen an eine der IP-Adressen des `localhost`. Secure Application Manager kapselt die Daten und sendet sie an das IVE. Das IVE entkapselt die Daten und sendet sie über Port 1494 an den passenden MetaFrame-Server.

Liste unterstützter Versionen

- MetaFrame™-Server: Versionen 1.8, XP 1.0, mit Service Packs 1 und 2
- Nfuse-Webserver: Versionen 1.5, 1.6 und 1.7
- ICA-Clients:
  - Windows 32-Bit: PN-Client Version 6.30 und Webclient Version 7,0
  - Benutzer von Program Neighborhood müssen den Server und die Anwendungen festlegen, auf die sie bei Verwendung des PN-Client zugreifen möchten. Diese Version des IVE unterstützt den

Suchmechanismus nicht, über den Anwendungen auf MetaFrame-Servern für Benutzer von Program Neighborhood angezeigt werden.

- Java: Version 6.2 für den eigenständigen Client und Versionen 6.2 und 6.3 für den Appletmodus. Wenn Sie den Appletmodus des Java-Client verwenden möchten, müssen Sie darauf achten, dass die Unterstützung für Java-Applets unter „Web > General page" aktiviert ist.

Hinweis:

Das IVE bietet eine Alternative zur Bereitstellung von CSG.

Teil 3
IVE-Konfiguration

In diesem Abschnitt finden Sie Informationen zur Konfiguration und Verwaltung von Access Series-Produkten.

Inhalt

Konfigurieren der Seite „Status“ 125
Konfigurieren der Seite „Schedule“ 136
Konfigurieren der Seite „Configuration“ 137
Konfigurieren der Seite „Network“ 157
Konfigurieren der Seite „Clustering“ 167
Protokollierung und Überwachung – Übersicht 95
Konfigurieren der Seite „Signing-in“ 203
Konfigurieren eines Authentifizierungsbereichs 273
Konfigurieren der Seite „Delegation“ 265
Konfigurieren der Seite „Roles“ 285
Konfigurieren der Seite „New User“ 323
Konfigurieren der Seite „Web“ 325
Konfigurieren der Seite „Files“ 351
Konfigurieren der Seite „SAM“ 361
Konfigurieren der Seite „Telnet/SSH“ 365
Konfigurieren der Seite „Network Connect“ 369
Konfigurieren der Seite „Meetings“ 375
Konfigurieren der Seite „Email Client“ 379
Konfigurieren der Seite „System“ 383
Konfigurieren der Seite „Import/Export“ 389
Konfigurieren der Seite „Push Config“ 399
Konfigurieren der Seite „Archiving“ 403
Konfigurieren der Seite „Troubleshooting“ 409

Konfigurieren der Seite „Status“

Die Seite **System > Status** enthält die folgenden Registerkarten:

Registerkarte „Overview“ 125
Registerkarte „Active Users“ 131
Registerkarte „Meeting Schedule“ 133

Auf der Seite **System > Status** können Sie die folgenden Aufgaben durchführen:

Anzeigen der Auslastung der Systemkapazität 126
Konfigurieren von Diagrammen zur Auslastung der Systemkapazität 128
Anzeigen kritischer Systemereignisse 128
Herunterladen des aktuellen Servicepakets 129
Bearbeiten von Systemdatum und -zeit 130
Überwachen von Benutzern mit Anmeldung am IVE 131
Anzeigen und Absagen geplanter Konferenzen 133

Registerkarte „Overview“

Wenn Sie sich an der Webkonsole anmelden, ist die Seite **System > Status** ausgewählt, und die Registerkarte **Overview** wird angezeigt. Auf dieser Registerkarte sind die Details zum IVE-Server und den Systembenutzern zusammengefasst. Wenn Sie auf anderen Seiten der Webkonsole Änderungen vornehmen, werden die entsprechenden Informationen auf der Seite **General** aktualisiert.

Hinweis: Diese Registerkarte ist die Startseite für alle Administratoren, d.h. auch für Administratoren mit delegierten Rechten ohne Lese- oder Schreibzugriff auf die Registerkarten unter **System > Status**.

Auf dieser Seite können Sie Folgendes ausführen:

Anzeigen der Auslastung der Systemkapazität 126
Konfigurieren von Diagrammen zur Auslastung der Systemkapazität 128
Anzeigen kritischer Systemereignisse 128
Herunterladen des aktuellen Servicepakets 129
Bearbeiten von Systemdatum und -zeit 130

☑ Anzeigen der Auslastung der Systemkapazität

Das Central Manager-Dashboard für Access Series- und Meeting Series-Appliances bietet Diagramme über die Auslastung der Systemkapazität, in denen Sie problemlos ablesen und übersehen können, wie hoch die Systemauslastung normalerweise ist. Um diese Informationen an anderen Stellen für Datenberichte zu verwenden, können Sie sie anhand der Optionen auf der Seite **Maintenance > Import/Export > Configuration** als XML-Datei exportieren.

Diese Diagramme werden in der geöffneten Webkonsole auf der Registerkarte **System > Status > Overview** angezeigt, und Sie können Folgendes leicht ablesen:

- **Concurrent Users**

  Dieses Diagramm zeigt die Anzahl von Benutzern an, die am IVE angemeldet sind. Bei einer Cluster-Umgebung werden im Diagramm zwei Linien angezeigt. Die erste Linie zeigt die Anzahl der lokalen Benutzer an, die an dem Knoten angemeldet sind, der in der Dropdownliste ausgewählt ist, und die zweite Linie zeigt die Anzahl der gleichzeitig am gesamten Cluster angemeldeten Benutzer an.

- **Concurrent Meetings (nur Secure Meeting-Appliance)**

  Dieses Diagramm zeigt die Anzahl der gegenwärtig stattfindenden Konferenzen an. Bei einer Cluster-Umgebung werden im Diagramm zwei Linien angezeigt. Die erste Linie zeigt die Anzahl der Konferenzen an, die auf dem Knoten stattfinden, der in der Dropdownliste ausgewählt ist, und die zweite Linie zeigt die Anzahl der gleichzeitig im gesamten Cluster stattfindenden Konferenzen an.

- **Hits Per Second**

  Dieses Diagramm zeigt die Anzahl der gegenwärtig vom IVE verarbeiteten Zugriffe an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden. Das Diagramm enthält vier Linien: Anzahl der Zugriffe, Anzahl der Webzugriffe, Anzahl der Dateizugriffe und Anzahl der Client/Server-Zugriffe.

- **CPU and Memory Usage**

  Dieses Diagramm zeigt den Prozentsatz der aktuellen CPU- und Speicherauslastung an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden.

- **Throughput**

  Dieses Diagramm zeigt die gegenwärtig verarbeitete Datenmenge (in KB) an. In einer Clusterumgebung legen Sie durch die Auswahl eines IVE aus der Dropdownliste den Knoten fest, dessen Daten im Diagramm angezeigt werden. Das Diagramm enthält vier Linien: extern ein, extern aus, intern ein und intern aus.

Im Fenster **Page Settings** können Sie festlegen, welche Diagramme das IVE im Dashboard anzeigt und für welchen Zeitraum das IVE die Daten verfolgt.

Abbildung 12: Seite „System > Status > Overview“

☑ Konfigurieren von Diagrammen zur Auslastung der Systemkapazität

So konfigurieren Sie Diagramme zur Auslastung der Systemkapazität:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Page Settings**.
3. Wählen Sie aus, welche Auslastungsdiagramme angezeigt werden sollen.
4. Wählen Sie den Zeitraum aus, der in den Diagrammen dargestellt werden soll. Die Intervalle können zwischen 1 Stunde und 1 Jahr liegen.
5. Geben Sie an, wie oft die Diagramme aktualisiert werden sollen.
6. Klicken Sie auf **Save Changes**.

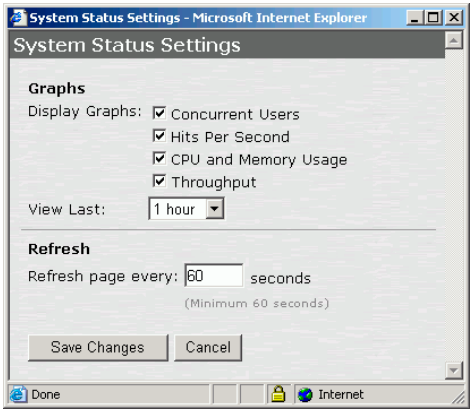


Abbildung 13: **Seite „System > Status > Overview > Page Settings “**

☑ Anzeigen kritischer Systemereignisse

Mit dem Central Manager-Dashboard für Access Series- und Meeting Series-Appliances können Sie ganz einfach die letzten zehn kritischen Systemereignisse anzeigen. Im Fenster **Event Monitor** können Sie schnell auf kritische Systemprobleme zugreifen und diese beheben. Während Sie in der Webkonsole Routineaufgaben zur Wartung und Konfiguration ausführen, können Sie das Fenster **Event Monitor** geöffnet lassen und die Systemereignisse überwachen.

So zeigen Sie schnell kritische Systemereignisse an:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Critical Events**. Im Fenster **Event Monitor** werden der Schweregrad und eine Meldung zu kritischen Ereignissen in der Systemprotokolldatei angezeigt.
3. Klicken Sie auf **Refresh**, um die neuesten Ereignisse anzuzeigen (optional).
4. Klicken Sie auf **See All** , um zur Registerkarte **System > Log/Monitoring > Events > Log** zu navigieren, auf der alle Ereignisse, von informativ bis kritisch, angezeigt werden (optional). Weitere Informationen finden Sie unter „Konfigurieren der Seite „Log Monitoring““ auf Seite 187.

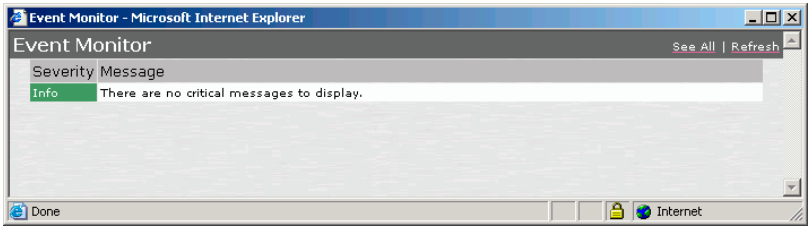


Abbildung 14: **Seite „System > Status > Overview > Critical Events“**

☑ Herunterladen des aktuellen Servicepakets

Auf der Registerkarte **System > Status > Overview** können Sie das Servicepaket herunterladen, dass zurzeit im IVE installiert ist, damit Sie es leicht speichern und auf einem anderen IVE installieren können.

So laden Sie das aktuelle Servicepaket herunter:

1. Wählen Sie in der Webkonsole **System > Status > Overviews** aus.
2. Klicken Sie auf **Download Package** (Central Manager-Version) oder auf die Verknüpfung neben **System Software Pkg Version** .
3. Klicken Sie auf **Speichern**.
4. Geben Sie einen Namen und einen Speicherort für das Servicepaket an.
5. Klicken Sie auf **Speichern**.

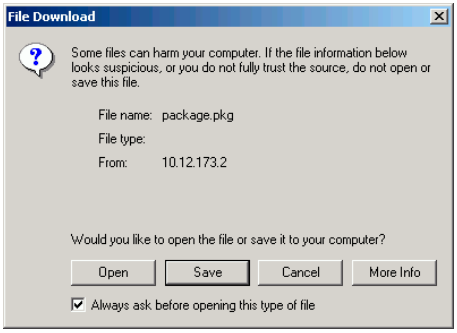

File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: package.pkg
File type:
From: 10.12.173.2
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

Abbildung 15: Seite „System > Status > Overview > Download Package“

☑ Bearbeiten von Systemdatum und -zeit

Sie müssen die Serverzeit einstellen, damit die Systemereignisse und die Übertragung von Benutzerdateien genau aufgezeichnet werden. Sie können das IVE über einen NTP-Server (Network Time Protocol) mit anderen Computern synchronisieren oder die IVE-Zeit manuell einrichten.

So bearbeiten Sie Systemdatum und -zeit:

1. Wählen Sie in der Webkonsole **System > Status > Overview** aus.
2. Klicken Sie im Abschnitt **System Date & Time** auf **Edit**.
3. Wählen Sie im Menü **Time Zone** eine Zeitzone aus. Das IVE passt die Uhrzeit automatisch an die Sommerzeit an.
4. Stellen Sie die Systemzeit mithilfe einer der folgenden Methoden ein:
   - **Use NTP server**

     Wählen Sie die Option **Use NTP Server** aus, geben Sie die IP-Adresse oder den Namen des Servers ein, und geben Sie ein Aktualisierungsintervall an.
   - **Set Time Manually**

     Wählen Sie die Option **Set Time Manually** aus, und geben Sie Werte für Datum und Uhrzeit ein. Sie können auch auf **Get from Browser** klicken, damit Daten in die Felder **Date** und **Time** eingegeben werden.
5. Klicken Sie auf **Save Changes**.

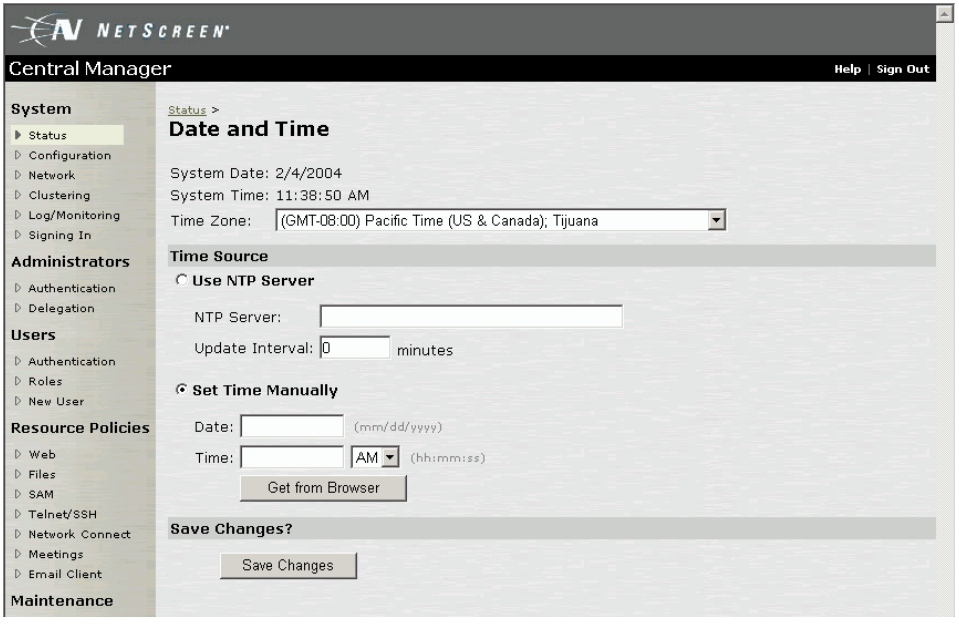


Abbildung 16: System > Status > Overview > Date and Time

Registerkarte „Active Users“

☑ Überwachen von Benutzern mit Anmeldung am IVE

Über das Menü **Active Users** können Sie Benutzer überwachen, die am IVE angemeldet sind. Dabei werden der Name jedes Benutzers, der Authentifizierungsbereich und die Anmeldezeit aufgeführt.

Hinweis: Das IVE zeigt für Nicht-IVE-Benutzer, die sich zur Teilnahme an einem Secure Meeting am IVE angemeldet haben, in den Spalten **Realm** und **Role** „N/A“ (keine Angabe) an.

So überwachen Sie am IVE angemeldete Benutzer:

1. Wählen Sie in der Webkonsole **System > Status > Active Users** aus.
2. Führen Sie bei Bedarf die folgenden Vorgänge durch:
   - **Abmelden von Benutzern von einer IVE-Sitzung:**
     - Um einen oder mehrere Endbenutzer oder Administratoren zwangsweise abzumelden, aktiveren Sie die Kontrollkästchen neben den entsprechenden Namen, und klicken Sie dann auf **Delete Session**.
     - Um alle aktuell angemeldeten Endbenutzer zwangsweise abzumelden, klicken Sie auf **Delete All Sessions**. (Beachten Sie, dass Sie Administratoren für die Abmeldung einzeln auswählen und die Schaltfläche **Delete Session** verwenden müssen.)
   - **Konfigurieren der angezeigten Daten und ihrer Reihenfolge:**
     - Geben Sie zum Anzeigen eines bestimmten Benutzers seinen Benutzernamen im Feld **Show Users Named** ein, und klicken Sie auf **Update**. Wenn Sie den genauen Benutzernamen nicht kennen, verwenden Sie einen Platzhalter (*). Wenn z.B. ein Benutzer „Joseph Jones" heißt, Sie sich aber nicht erinnern können, ob der Benutzername „Joe" oder „Joseph" lautet, geben Sie im Feld **Show Users Named** die Zeichenfolge „Jo*" ein Das IVE gibt eine Liste aller Benutzer zurück, deren Benutzername mit den Buchstaben „jo" beginnt.
     - Um zu steuern, wie viele Benutzer und Administratoren auf der Seite **Active Users** angezeigt werden, geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**.
     - Um die Tabelle der aktuell angemeldeten Benutzer und Administratoren zu sortieren, klicken Sie auf eine Spaltenüberschrift.
     - Klicken Sie zum Aktualisieren des Seiteninhalts auf **Update**.
   - **Erstellen einer Verknüpfung mit weiteren Registerkarten:**
     - Klicken Sie zum Bearbeiten des Authentifizierungsbereichs eines Benutzers neben dem Namen auf die Verknüpfung **Realm**, und folgen Sie den Anweisungen unter „Konfigurieren eines Authentifizierungsbereichs" auf Seite 273.
     - Klicken Sie zum Bearbeiten der Rolle eines Benutzers auf die Verknüpfung **Role** neben seinem Namen, und folgen Sie den Anweisungen unter „Konfigurieren der Seite „Delegation"" auf Seite 265 (für Administratoren) oder „Konfigurieren der Seite „Roles"" auf Seite 285 (für Endbenutzer).

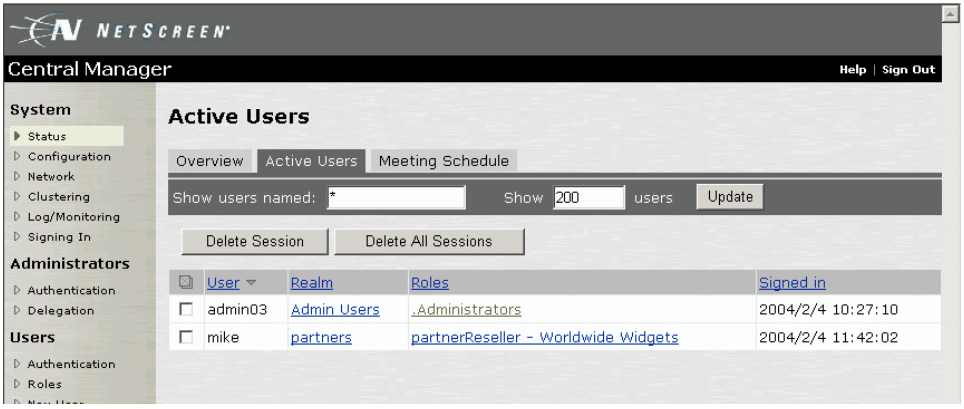


Abbildung 17: System > Status > Active Users

Registerkarte „Meeting Schedule“

☑ Anzeigen und Absagen geplanter Konferenzen

Zeigen Sie mit den Seiten **Meeting Schedule** (Access Series-Appliance) oder **Schedule** (Meeting Series-Appliance) alle gegenwärtig auf dem IVE geplanten Konferenzen an, und sagen Sie ggf. Konferenzen ab.
(Eine Beschreibung der Option „Secure Meeting“ finden Sie unter „Secure Meeting – Übersicht“ auf Seite 13.)

So zeigen Sie geplante Konferenzen an oder sagen diese ab:

1. Wählen Sie in der Webkonsole **System > Status > Meeting Schedule** (Access Series-Appliance) oder **System > Schedule** (Meeting Series-Appliance) aus. Das IVE zeigt Echtzeitinformationen zu allen gegenwärtig ausgeführten oder geplanten Konferenzen an, einschließlich:
   - **Time and Status**

     Zeigt die geplante Zeit und Dauer der Konferenz sowie den aktuellen Status an.
   - **Meeting Details**

     Zeigt den Konferenznamen sowie ID- und Kennwortanforderungen an. Diese Spalte enthält außerdem eine Verknüpfung **Details**, über die Sie Informationen zur Konferenz und Konferenzteilnahme anzeigen können.

- **Meeting Role**

  Zeigt die Rolle des Konferenzerstellers an. Wenn der Ersteller beim Erstellen der Konferenz unter mehreren Rollen angemeldet war (wenn er z. B. Mitglied mehrerer Rollen ist und die Appliance für eine permissive Zusammenführung konfiguriert ist), wählt Secure Meeting eine Rolle aus, wie unter „Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen“ auf Seite 318 dargestellt.

- **Attendee Roles**

  Zeigt die Rollen der für die Konferenz angemeldeten Teilnehmer, die Anzahl der für jede Rolle angemeldeten Teilnehmer und die Teilnehmerobergrenze für jede Rolle an. Informationen darüber, wie Teilnehmer zu Rollen zugewiesen und wie Obergrenzen für eine Rolle festgelegt werden, finden Sie unter „Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen“ auf Seite 318.

2. Mithilfe der folgenden Methoden können Sie die Konferenzansicht ändern (optional):
   - Wählen Sie aus den Gruppenregisterkarten (Meeting Series-Appliance) oder in der Dropdownliste (Access Series-Appliance) einen Zeitrahmen aus (**Daily**, **Weekly**, **In Progress** oder **Scheduled**), um festzulegen, welche Konferenzen angezeigt werden.
   - Klicken Sie auf eine beliebige unterstrichene Spaltenüberschrift, um die Sortierreihenfolge der derzeit angezeigten Konferenzen zu steuern.
3. Klicken Sie unterhalb einer Konferenz auf die Verknüpfung **Details**, um Informationen zur Konferenz anzuzeigen und dieser ggf. beizutreten (optional).
4. Klicken Sie auf das Löschsymbol in der rechten Spalte, um eine Konferenz abzusagen (optional).

Wichtig: Durch das Absagen wird eine Konferenz endgültig aus dem IVE gelöscht. Sie können eine Konferenz nach dem Absagen nicht wiederherstellen.

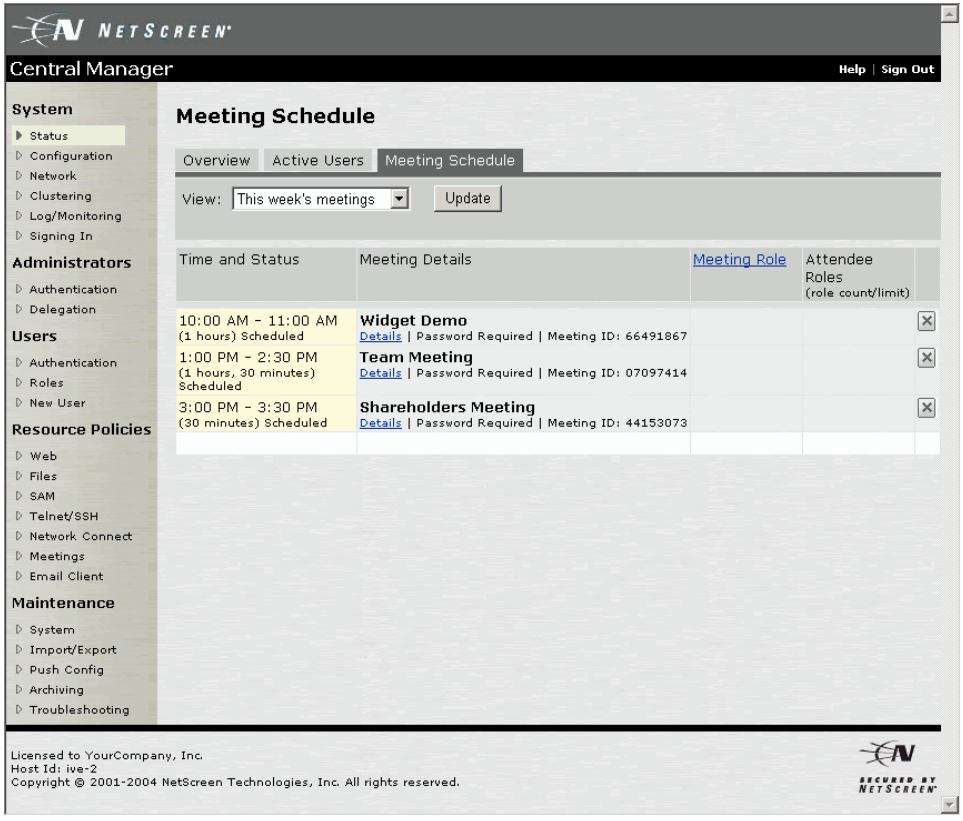


Abbildung 18: System > Status > Meeting Schedule

Konfigurieren der Seite „Schedule“

Auf der Seite **Schedule** (Meeting Series-Appliance) können Sie alle gegenwärtig auf dem IVE geplanten Konferenzen anzeigen und Konferenzen ggf. absagen. Weitere Informationen finden Sie unter „Registerkarte „Meeting Schedule““ auf Seite 133.

Konfigurieren der Seite „Configuration“

Die Seite **System > Configuration** enthält die folgenden Registerkarten:

Registerkarte „Licensing“ 137
Registerkarte „Security > Security Options“ 140
Registerkarte „Security > Host Checker“ 143
Registerkarte „Security > Cache Cleaner“ 146
Registerkarte „Certificates > Server Certificate“ 147
Registerkarte „Certificates > CA Certificate“ 153
Registerkarte „Certificates > Applet Certificates“ 155

Auf der Seite **System > Configuration** können Sie die folgenden Aufgaben durchführen:

Eingeben oder Aktualisieren einer IVE-Lizenz 138
Festlegen von systemweiten Sicherheitsoptionen 140
Erstellen einer globalen Hostprüfung-Richtlinie 143
Angeben globaler Einstellungen für die Cachebereinigung 146
Importieren eines vorhandenen Serverzertifikats und eines privaten Schlüssels 147
Importieren eines erneuerten Serverzertifikats, das den vorhandenen privaten Schlüssel verwendet 150
Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat 151
Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde 152
Importieren eines Stammzertifikats zur Überprüfung clientseitiger Zertifikate 153
Importieren eines Codesignaturzertifikats 155

Registerkarte „Licensing“

Das IVE enthält eine Lizenz für den Standardzugriff auf das IVE[1]. Um das System im vollen Umfang nutzen zu können, müssen Sie sich jedoch an der Webkonsole anmelden und die Lizenzen eingeben, die Sie per E-Mail von NetScreen erhalten haben. Die E-Mail kann bis zu drei unterschiedliche Arten von Lizenzen enthalten:

- ***Produktlizenz*** – Eine Produktlizenz bestimmt die Anzahl von IVEs in einem Cluster sowie die Anzahl von Benutzern, die sich gleichzeitig beim

1. Mit der grundlegenden IVE-Lizenz können Sie fünf lokale Benutzerkonten erstellen, zwei Benutzer können sich gleichzeitig anmelden, und es werden grundlegende Funktionen zum Navigieren durch Web-, Windows- und UNIX/NFS-Dateien bereitgestellt.

System anmelden können. Ihre Produktlizenz kann z.B. erlauben, dass Sie einen 4-Unit-Cluster aus A5000-Einheiten mit 2.500 Benutzern erstellen, die gleichzeitig zugreifen können.

- ***Lizenz für Aktualisierungspakete –*** Mit einer Lizenz für Aktualisierungspakete können Sie eine Reihe von Features verwenden. Wenn Sie über eine Central Manager-Lizenz verfügen, können Sie verschiedene Funktionen verwenden: IVE-Dashboard-Funktion zum Überwachen der Systemkapazität, Konfigurationsübertragungsfunktion zum Übernehmen der Einstellungen aus einem IVE in ein anderes, Funktion für ausfallfreie Aktualisierungen zum Beschleunigen von Aktualisierungen, Sicherungsfunktion zum lokalen Speichern von Sicherungsdateien und Protokollberichtsfunktion zum Anpassen des Protokolldateiformats.
- ***Lizenz für die Aktualisierungsfunktion*** – Mit einer Lizenz für die Aktualisierungsfunktion können Sie eine einzelne Funktion verwenden. Mit einer Secure Terminal-Lizenz können Sie z.B. von jedem Benutzercomputer aus über Telnet oder SSH auf gehostete Server sicher zugreifen.

Geben Sie mithilfe der Registerkarte **System > Configuration > Licensing** die Lizenzcodes für Ihre Site ein, zeigen Sie die Ablaufdaten ein, und löschen Sie diese ggf.

Hinweis: Lesen Sie in jedem Fall die Lizenzvereinbarung, auf die Sie über die Registerkarte **Licensing** zugreifen können, bevor Sie Ihre Lizenz senden. Bei der über die Registerkarte **Licensing** verfügbaren Lizenzvereinbarung handelt es sich um denselben Text, der während des ersten Setups an der seriellen Konsole angezeigt wird.

☑ Eingeben oder Aktualisieren einer IVE-Lizenz

So geben Sie die IVE-Lizenz ein oder aktualisieren diese:

1. Wählen Sie in der Webkonsole **System > Configuration > Licensing** aus.
2. Klicken Sie auf die Verknüpfung **License Agreement**. Lesen Sie die Lizenzvereinbarung. Wenn Sie mit den Bestimmungen einverstanden sind, fahren Sie mit dem nächsten Schritt fort.
3. Geben Sie den Firmennamen und den Lizenzschlüssel ein, und klicken Sie dann auf **Save changes**.

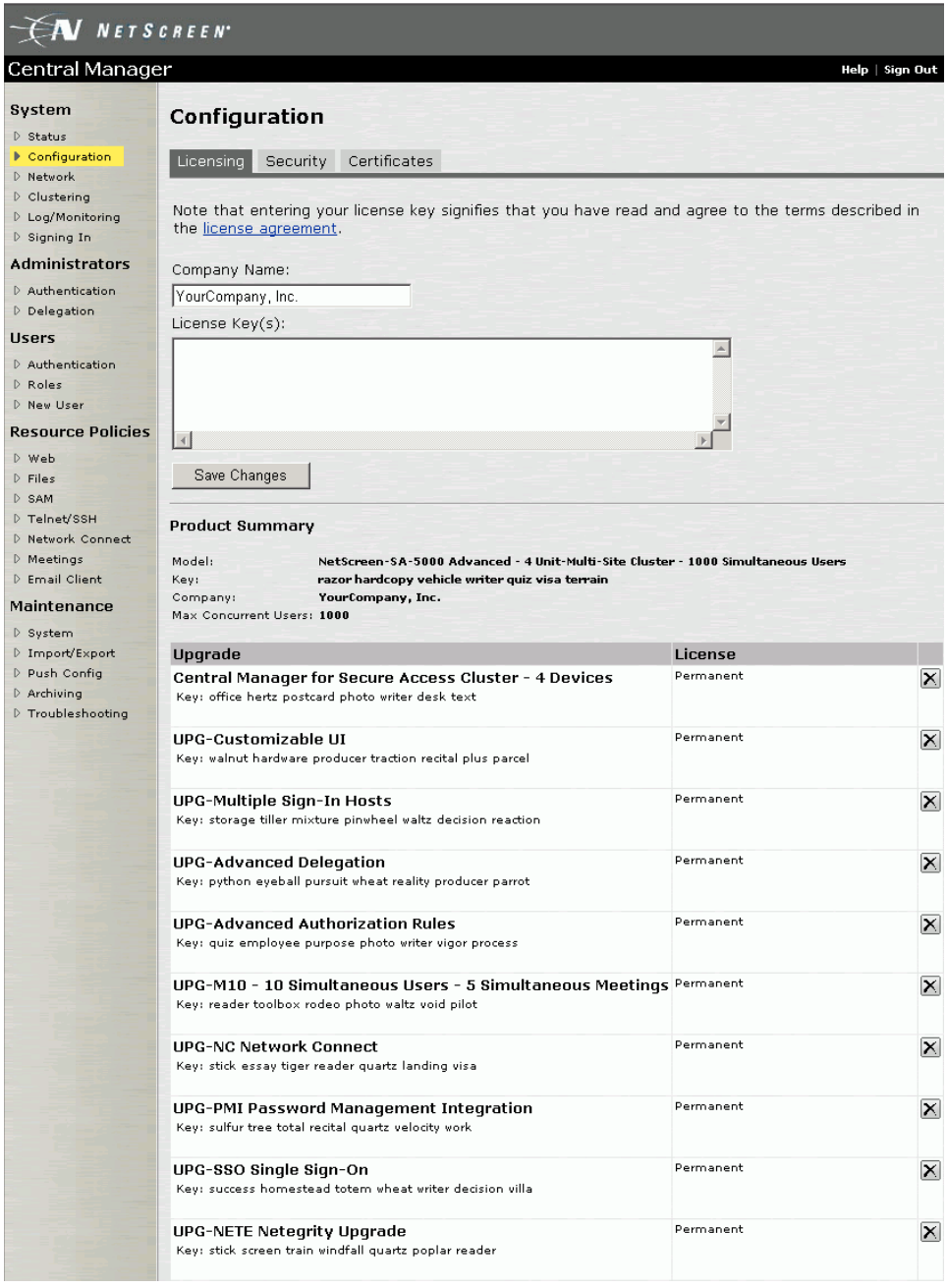


Abbildung 19: System > Configuration > Licensing

Registerkarte „Security > Security Options“

Mit der Registerkarte **System > Configuration > Security > Security Options** können Sie die Standardsicherheitseinstellungen für das IVE festlegen. Wir empfehlen, die Standardsicherheitseinstellungen zu verwenden, die höchste Sicherheit gewährleisten. Falls die Benutzer bestimmte Browser jedoch nicht verwenden oder auf bestimmte Webseiten nicht zugreifen können, müssen Sie diese Einstellungen jedoch möglicherweise ändern.

☑ Festlegen von systemweiten Sicherheitsoptionen

Wenn bei Benutzern beim Zugriff auf bestimmte Webseiten Browserprobleme auftreten, müssen Sie ggf. Folgendes anpassen:

- **Zulässige SSL- bzw. TLS-Version**

  Für den NetScreen IVE-Server sind standardmäßig SSL, Version 3, und TLS erforderlich. In älteren Browsern wird SSL, Version 2, verwendet. Sie können entweder die Benutzer ihre Browser aktualisieren lassen oder die Einstellung ändern, damit sowohl SSL, Version 2, als auch SSL, Version 3, zulässig sind.

- **Zulässige Verschlüsselungsstärke**

  Für den NetScreen IVE-Server ist standardmäßig 128-Bit-Verschlüsselung erforderlich. Sie können außerdem angeben, dass für das IVE 168-Bit-Verschlüsselung erforderlich ist. In älteren Browsern, die vor der Änderung des US-Exportgesetzes im Jahr 2000 entwickelt wurden, das bis dahin für den internationalen Export eine Verschlüsselungsstärke von 40 Bit vorschrieb, wird u.U. noch die 40-Bit-Verschlüsselung verwendet. Sie können entweder den Benutzern mitteilen, dass diese eine Aktualisierung auf einen Browser mit 128-Bit-Verschlüsselung vornehmen sollen, oder die erforderliche Verschlüsselungsstärke ändern, sodass auch die 40-Bit-Verschlüsselung zulässig ist.

- **Navigation zu SSL-Sites**

  Der NetScreen IVE-Server gestattet die Navigation zu internen SSL-Sites (denen https:// vorangestellt ist) und akzeptiert als Standard sämtliche (temporären oder anderen) Zertifikate. Falls Sie Bedenken wegen Benutzern haben, die über das IVE zu Sites ohne Zertifikate von einer gültigen externen Zertifizierungsstelle navigieren, deaktivieren Sie diese Funktion.

- **Vermittlung der Standardauthentifizierung**

  Der NetScreen Instant Virtual Extranet-Server kann die Anmeldeinformationen von Benutzern vermitteln, um zu verhindern, dass ein Benutzer über die zwischengespeicherten Anmeldeinformationen eines anderen Benutzers auf Ressourcen zugreifen kann. Darüber hinaus kann das IVE die Anmeldeinformationen von Benutzern wiederverwenden und ermöglicht somit die Einzelanmeldung (Single Sign-In) für andere Intranetsites.

Wenn Sie die Option für die Einzelanmeldung auswählen, stellt das IVE sicher, dass die Anmeldeinformationen nur innerhalb des Firmenintranets weitergeleitet werden.

- **NetScreen Communication Protocol (NCP) für Client-Server-Anwendungen**

  Das Instant Virtual Extranet verwendet das NetScreen Communication Protocol (NCP) für die Kommunikation zwischen dem IVE-Server und einigen Clientanwendungen, z.B. Secure Meeting, W-SAM (Windows-Version des Secure Application Manager) und Network Connect. Das IVE kann zwei Versionen dieses Protokolls verwenden, optimiertes NCP (oNCP) und Standard-NCP. Wenn Sie **Auto-select Enabled** auswählen, optimiert das IVE die Systemleistung, indem es für einen Großteil der Client/Server-Kommunikation oNCP verwendet und ggf. zu Standard-NCP wechselt[1].

1. Das IVE verwendet hauptsächlich dann Standard-NCP, wenn keine direkte Socketverbindung hergestellt werden kann (im Allgemeinen weil ein Proxy vorhanden ist).

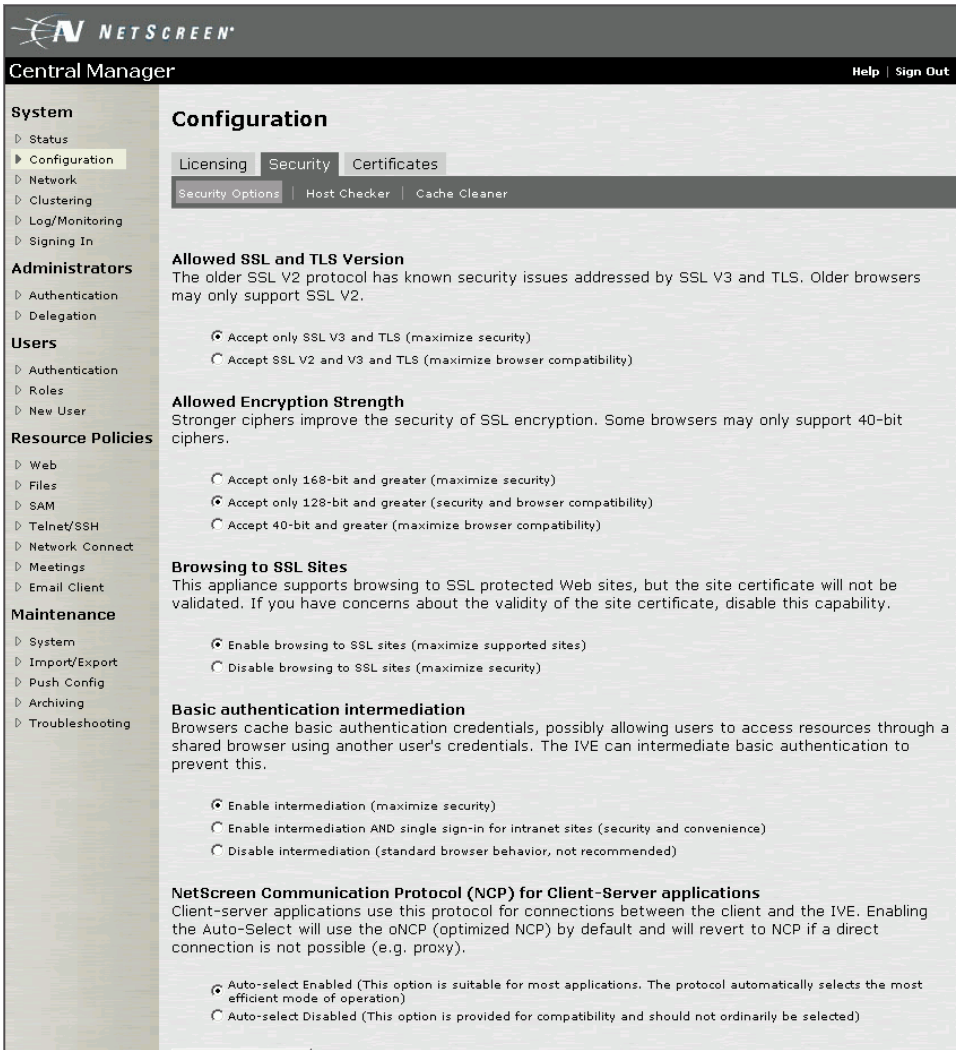

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Configuration
Licensing
Security
Certificates
Security Options
Host Checker
Cache Cleaner
Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. Older browsers may only support SSL V2.
Accept only SSL V3 and TLS (maximize security)
Accept SSL V2 and V3 and TLS (maximize browser compatibility)
Allowed Encryption Strength
Stronger ciphers improve the security of SSL encryption. Some browsers may only support 40-bit ciphers.
Accept only 168-bit and greater (maximize security)
Accept only 128-bit and greater (security and browser compatibility)
Accept 40-bit and greater (maximize browser compatibility)
Browsing to SSL Sites
This appliance supports browsing to SSL protected Web sites, but the site certificate will not be validated. If you have concerns about the validity of the site certificate, disable this capability.
Enable browsing to SSL sites (maximize supported sites)
Disable browsing to SSL sites (maximize security)
Basic authentication intermediation
Browsers cache basic authentication credentials, possibly allowing users to access resources through a shared browser using another user's credentials. The IVE can intermediate basic authentication to prevent this.
Enable intermediation (maximize security)
Enable intermediation AND single sign-in for intranet sites (security and convenience)
Disable intermediation (standard browser behavior, not recommended)
NetScreen Communication Protocol (NCP) for Client-Server applications
Client-server applications use this protocol for connections between the client and the IVE. Enabling the Auto-Select will use the oNCP (optimized NCP) by default and will revert to NCP if a direct connection is not possible (e.g. proxy).
Auto-select Enabled (This option is suitable for most applications. The protocol automatically selects the most efficient mode of operation)
Auto-select Disabled (This option is provided for compatibility and should not ordinarily be selected)

Abbildung 20: System > Configuration > Security > Security Options

Registerkarte „Security > Host Checker“

Auf der Registerkarte **System > Configuration > Security> Hostprüfung** können Sie globale Hostprüfung-Richtlinien erstellen, die dann für Authentifizierungsrichtlinien (für Authentifizierungsbereiche), Rollenzuordnungsregeln und Ressourcenrichtlinien zur Verfügung stehen. Weitere Informationen finden Sie unter „Hostprüfung – Übersicht“ auf Seite 91.

☑ Erstellen einer globalen Hostprüfung-Richtlinie

So erstellen Sie eine globale Hostprüfung-Richtlinie:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Host Checker** aus.
2. Geben Sie auf der Registerkarte **Security > Host Checker** einen Namen für die Hostprüfung-Richtlinie an, und klicken Sie dann auf **Continue**.
3. Wählen Sie unter **Host Checking Method** eine beliebige Anzahl der folgenden Optionen aus:
   - **Sygate Enforcement API**

     Zur Verwendung dieser Option muss das Produkt Sygate Personal Firewall auf dem Clientcomputer installiert sein.
   - **Sygate Security Agent**

     Zur Verwendung dieser Option muss Sygate Security Agent auf dem Clientcomputer installiert sein.
   - **Zone Labs: Zone Alarm Pro und Zone Labs Integrity**

     Zur Verwendung dieser Option muss entweder Zone Alarm Pro oder Zone Labs Integrity auf dem Clientcomputer installiert sein.
   - **McAfee Desktop Firewall 8.0**

     Zur Verwendung dieser Option muss McAfee Desktop Firewall 8.0 auf dem Clientcomputer installiert sein.
   - **InfoExpress CyberGatekeeper Agent**

     Zur Verwendung dieser Option muss InfoExpress CyberGatekeeper Agent auf dem Clientcomputer installiert sein.
4. Erstellen Sie unter **Rule Settings** Regeln, die von der Hostprüfung durchgesetzt werden sollen:
   1. Wählen Sie einen Regeltyp aus der Dropdownliste aus, und klicken Sie anschließend auf **Add**. (Beschreibungen hierzu finden Sie unter „Erstellen globaler Richtlinien für die Hostprüfung“ auf Seite 91.)
   2. Geben Sie im Dialogfeld **Add Attribute Check** die erforderlichen Informationen für die Regel ein:

- **Custom NHC Integration** – geben Sie einen Namen für die DLL und den Speicherort der DLL auf Clientcomputern (Pfad und Dateiname) ein.
- **Attribute Check: Ports** – geben Sie eine Liste von Ports mit Kommas als Trennzeichen oder einen Bereich von Ports ein, beispielsweise: `1234, 11000-11999, 1235`. Wählen Sie **Required** aus, um zu fordern, dass diese Ports auf dem Clientcomputer geöffnet sind, oder wählen Sie **Deny** aus, um zu fordern, dass sie geschlossen sind.
- **Attribute Check: Process** – geben Sie den Namen eines Prozesses (ausführbare Datei) ein, beispielsweise: `good-app.exe`. Wählen Sie **Required** aus, um zu fordern, dass dieser Prozess im Task-Manager ausgeführt wird, oder wählen Sie **Deny** aus, um zu fordern, dass dieser Prozess nicht ausgeführt wird. Sie können darüber hinaus den MD5-Prüfsummenwert der ausführbaren Datei angeben.
- **Attribute Check: File** – geben Sie den Namen einer Datei (eines beliebigen Dateityps) ein, beispielsweise: `\Temp\Bad-file.doc`. Wählen Sie **Required** aus, um zu fordern, dass diese Datei auf dem Clientcomputer vorhanden ist, oder wählen Sie **Deny** aus, um zu fordern, dass diese Datei nicht vorhanden ist. Sie können darüber hinaus den MD5-Prüfsummenwert dieser Datei angeben.
- **Attribute Check: Registry Setting** – geben Sie die Registrierungswerte ein, die auf dem Clientcomputer vorhanden sein sollen. Folgende Optionen stehen zur Verfügung:
- **Registry Root Key** – Wählen Sie einen Stammschlüssel aus der Dropdownliste aus. (Erforderlich.)
- **Registry Subkey** – Geben Sie den Pfad zum Anwendungsordner an. (Erforderlich.)
- **Name** – Der Name des Schlüsselwertes, der gefordert werden soll. Dieser Name wird in der Spalte **Name** des Registrierungs-Editors angezeigt. (Optional.)
- **Type** – Der Typ des Schlüsselwertes: Zeichenfolge, Binärwert oder DWORD. Dieser Typ wird in der Spalte **Type** des Registrierungseditors angezeigt. (Optional.)
- **Value** – Der Wert des Schlüsselwertes. Diese Informationen werden in der Spalte **Data** des Registrierungseditors angezeigt. (Optional.)

Hinweis: Wenn lediglich der Schlüssel und der Teilschlüssel angegeben werden, überprüft die Hostprüfung einfach das Vorhandensein des Ordners „Subkey“ in der Registrierung.

---

3 Klicken Sie im Dialogfeld auf **Save Changes**.

5. Klicken Sie auf der Seite Hostprüfung **Configuration** auf **Save Changes**, um die Hostprüfungs-Richtlinie zu erstellen.

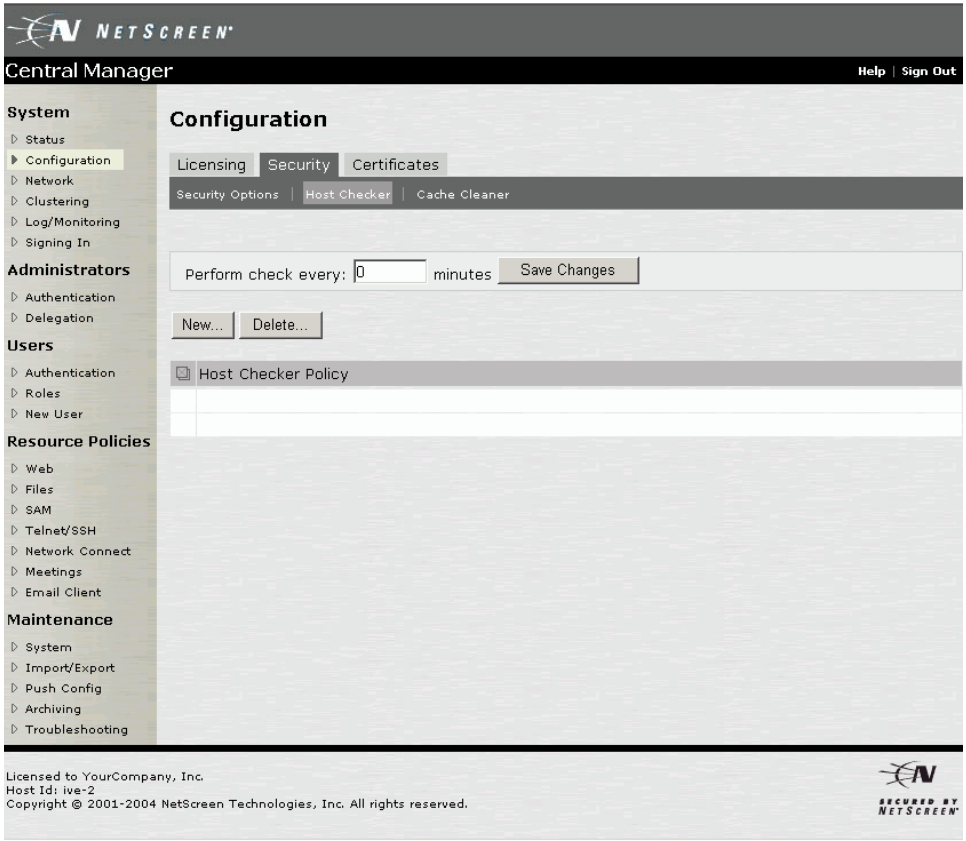


Abbildung 21: System > Configuration > Security > Host Checker

Registerkarte „Security > Cache Cleaner“

Auf der Registerkarte **System > Configuration > Security > Cachebereinigung** können Sie angeben, wie oft die Cachebereinigung ausgeführt und der IVE-Status aktualisiert wird. Weitere Informationen finden Sie unter „Cachebereinigung – Übersicht“ auf Seite 63.

☑ Angeben globaler Einstellungen für die Cachebereinigung

So geben Sie globale Einstellungen für die Cachebereinigung an:

1. Wählen Sie in der Webkonsole **System > Configuration > Security > Cachebereinigung** aus.
2. Geben Sie auf der Registerkarte **Security > Cachebereinigung** Folgendes an:
   - **Cleaner Frequency** – gibt an, wie oft die Cachebereinigung ausgeführt wird.
   - **Status Update Frequency** – gibt an, wie oft das IVE erwartet, dass die Cachebereinigung sich selbst aktualisiert.
3. Klicken Sie auf der Seite Cachebereinigung **Configuration** auf **Save Changes**, um diese Einstellungen global zu speichern.

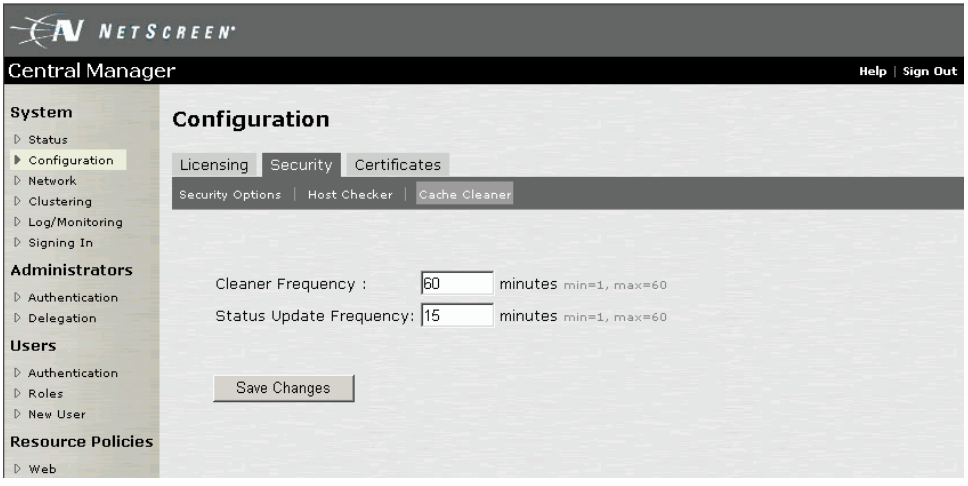


Abbildung 22: System > Configuration > Security > Cache Cleaner

Registerkarte „Certificates > Server Certificate“

Auf der Registerkarte **System > Configuration > Certificates > Server Certificate** können Sie eine Datei mit einem digitalen Serverzertifikat und dem entsprechenden Schlüssel auf das IVE importieren. Ein ***Serverzertifikat*** sichert den Netzwerkverkehr von und zu dem IVE. Wenn Ihr Unternehmen bereits über ein digitales Serverzertifikat verfügt, importieren Sie die Zertifikatsdatei und den entsprechenden Schlüssel in das IVE. Auf dieser Registerkarte können Sie auch ein auf dem vorhandenen privaten Schlüssel basierendes erneuertes Zertifikat importieren oder ein Zertifikat importieren, das auf einer Zertifikatssignaturanforderung basiert, die Sie an eine Zertifizierungsstelle gesendet haben. Weitere Informationen finden Sie unter „Serverzertifikate“ auf Seite 69.

Dieser Abschnitt umfasst folgende Aufgaben:

Importieren eines vorhandenen Serverzertifikats und eines privaten Schlüssels 147
Importieren eines erneuerten Serverzertifikats, das den vorhandenen privaten Schlüssel verwendet 150
Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat 151
Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde 152

☑ Importieren eines vorhandenen Serverzertifikats und eines privaten Schlüssels

Sie können Webserverzertifikate von Servern wie Apache, IIS, Sun ONE (früher iPlanet) oder Netscape erstellen und das Zertifikat dann in das IVE importieren. Zum Exportieren eines digitalen Serverzertifikats und eines Schlüssels folgen Sie den Anweisungen zum Exportieren von Zertifikaten für Ihren Webserver.

Wichtig: Beachten Sie beim Importieren eines Zertifikats, dass es verschlüsselt sein muss und dass Sie das Kennwort mit dem Zertifikat exportieren müssen. Beachten Sie außerdem, dass Sie den privaten Schlüssel für das Zertifikat eines Webservers nicht auf ein Access Series FIPS-Gerät importieren können, da der Schlüssel in einer Umgebung erstellt wird, die nicht FIPS-kompatibel ist. Sie können jedoch einen Zertifikatsschlüssel zusammen mit der Security World von einem anderen NetScreen IVE Access Series-Gerät impotieren. Weitere Informationen finden Sie unter „Importieren einer Systemkonfigurationsdatei“ auf Seite 390.

So importieren Sie ein vorhandenes digitales Serverzertifikat und einen privaten Schlüssel:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates** > **Server Certificate** aus.
2. Klicken Sie auf **Import / Renew**.
3. Wählen Sie das entsprechende Formular für den Import des Zertifikats aus:
   - Falls sich das Zertifikat und der Schlüssel in einer Datei befinden, verwenden Sie das Formular **Certificate file includes private key**.
   - Handelt es sich bei dem Zertifikat und dem Schlüssel um separate Dateien, verwenden Sie das Formular **Certificate and private key are separate files**.
4. Wechseln Sie im entsprechenden Formular zu der Datei mit dem Zertifikat und dem Schlüssel. Wenn die Datei verschlüsselt ist, geben Sie den Kennwortschlüssel ein.
5. Klicken Sie auf **Import**.

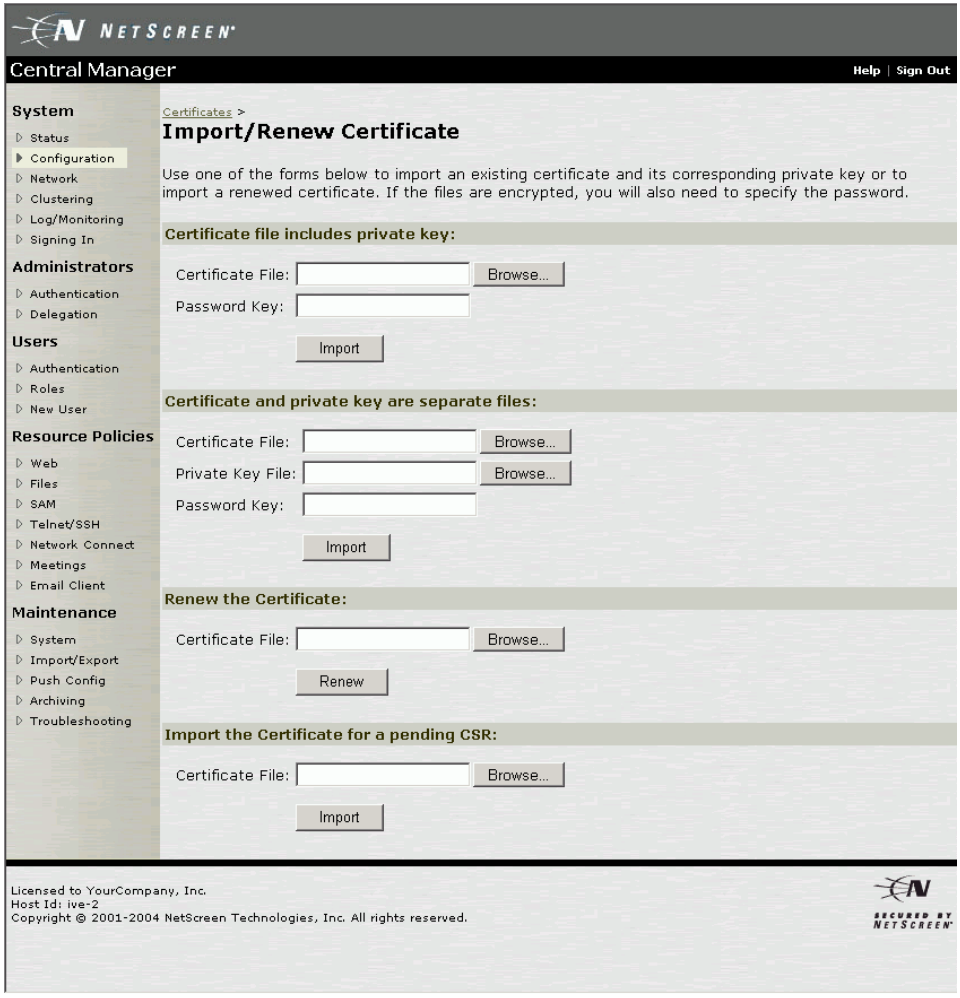


Abbildung 23: System > Configuration > Certificates > Server Certificates > Import/Renew

☑ Importieren eines erneuerten Serverzertifikats, das den vorhandenen privaten Schlüssel verwendet

Sie können ein Serverzertifikat auf zwei Arten erneuern:

- **Bei einer Zertifizierungsstelle eine neue Zertifikatssignaturanforderung einreichen**

  Dieser Vorgang zur Erneuerung eines Zertifikats ist sicherer, da die Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel generiert und dabei die Gültigkeit des älteren privaten Schlüssels aufhebt. Zur Verwendung dieser Erneuerungsmethode müssen Sie zuerst über die Webkonsole eine Zertifikatssignaturanforderung erstellen. Weitere Informationen finden Sie unter „Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat“ auf Seite 151.

  Wichtig: Sie können den privaten Schlüssel eines Webserverzertifikats nicht auf ein Access Series FIPS-Gerät importieren, da dieser Schlüssel in einer Umgebung erzeugt wird, die nicht mit FIPS kompatibel ist.

- **Basierend auf der vorher bei der Zertifizierungsstelle eingereichten Zertifikatssignaturanforderung eine Erneuerung anfordern**

  Dieser Vorgang zur Erneuerung eines Zertifikats ist weniger sicher, da die Zertifizierungsstelle ein Zertifikat generiert, das den vorhandenen privaten Schlüssel verwendet.

  Wichtig: Geben Sie bei der erneuten Anforderung eines Zertifikats dieselben Informationen an, die in der ursprünglichen Zertifikatssignaturanforderung verwendet wurden. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem vorhandenen Schlüssel entspricht.

So importieren Sie ein erneuertes Serverzertifikat, das den vorhandenen privaten Schlüssel verwendet:

1. Befolgen Sie die Anweisungen der Zertifizierungsstelle zur Erneuerung eines Zertifikats, das Sie zuvor dort erworben haben.

   Wichtig: Vergewissern Sie sich, dass Sie dieselben Informationen angeben, die in der ursprünglichen Zertifikatssignaturanforderung verwendet wurden. Anhand dieser Informationen erstellt die Zertifizierungsstelle ein neues Zertifikat, das dem vorhandenen Schlüssel entspricht.

2. Wählen Sie in der Webkonsole **System > Configuration > Certificates** > **Server Certificate** aus.
3. Klicken Sie auf **Import / Renew**.

4. Navigieren Sie über das Formular **Renew the Certificate** zu der Datei mit dem erneuerten Zertifikat, und klicken Sie dann auf **Renew** (**Abbildung 23** auf Seite 149).

☑ Erstellen einer Zertifikatssignaturanforderung für ein neues Serverzertifikat

Falls Ihr Unternehmen über kein digitales Zertifikat für die Webserver verfügt oder Sie ein Access Series FIPS-Gerät betreiben, können Sie über die Webkonsole eine Zertifikatssignaturanforderung (CSR) erstellen und diese dann zur Verarbeitung an eine Zertifizierungsstelle senden. Wenn Sie über die Webkonsole eine Zertifikatssignaturanforderung erstellen, wird lokal ein privater Schlüssel erstellt, der der Zertifikatssignaturanforderung entspricht. Wenn Sie die Zertifikatssignaturanforderung löschen, wird diese Datei ebenfalls gelöscht. Es ist dann nicht mehr möglich, ein über die Zertifikatssignaturanforderung erstelltes signiertes Zertifikat zu installieren.

Wichtig: Senden Sie nur jeweils eine Zertifikatssignaturanforderung an eine Zertifizierungsstelle. Andernfalls fallen u.U. doppelte Gebühren an. Sie können Details zu zuvor gesendeten, ausstehenden Anforderungen anzeigen, indem Sie auf die Verknüpfung **Certificate Signing Request Details** auf der Registerkarte **Server Certificates** klicken.

So erstellen Sie eine Zertifikatssignaturanforderung:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > Server Certificate** aus.
2. Klicken Sie unter **Pending Certificate Signing Request** auf **New CSR**.
3. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Create CSR**.
4. Folgen Sie den Anweisungen auf dem Bildschirm. Darin wird neben dem Sendeverfahren erläutert, welche Informationen an die Zertifizierungsstelle gesendet werden müssen. Wenn Sie von der Zertifizierungsstelle ein signiertes Zertifikat erhalten, importieren Sie die Zertifikatdatei. Befolgen Sie dabei die unter „Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde“ auf Seite 152 angegebenen Anweisungen.

Hinweis: Wenn Sie eine Zertifikatssignaturanforderung bei einer Zertifizierungsstelle einreichen, werden Sie u. U. dazu aufgefordert, entweder den Typ des Webservers anzugeben, auf dem das Zertifikat erstellt wurde, oder den Typ des Webservers, für den das Zertifikat bestimmt ist. Wählen Sie **apache_modssl** aus. (Falls mehrere Optionen mit „apache_modssl“ verfügbar sind, können Sie eine beliebige auswählen.) Wählen Sie außerdem, falls Sie zur Auswahl des Formats des herunterzuladenden Zertifikats aufgefordert werden, das Standardformat aus.

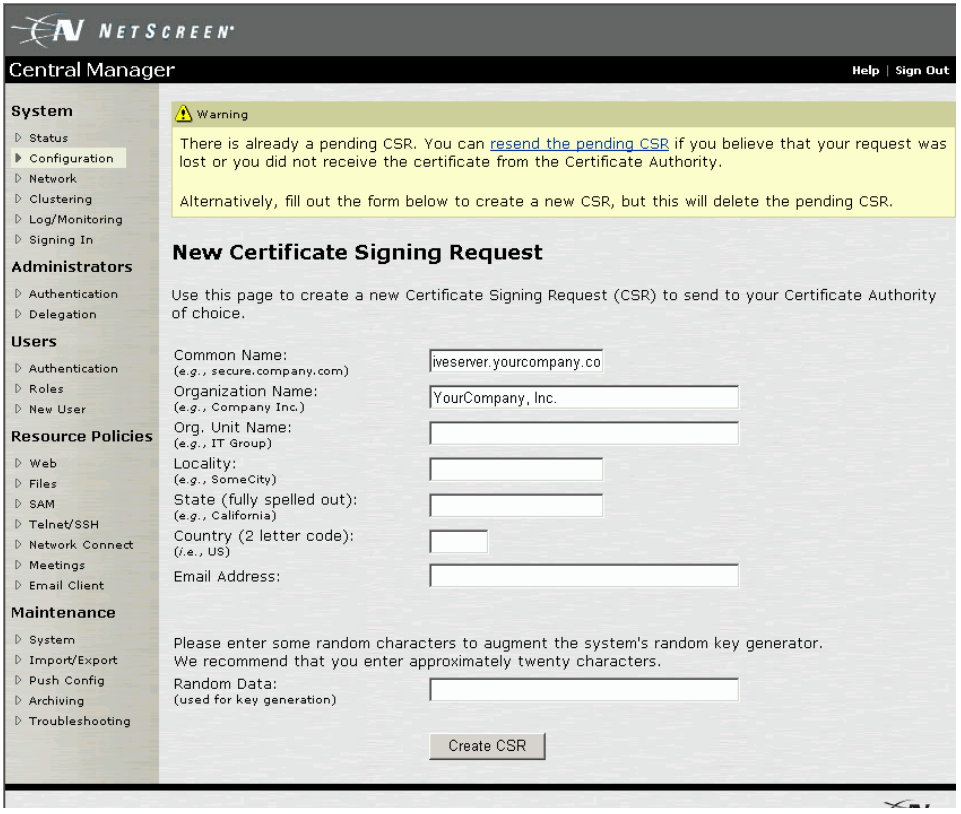


Abbildung 24: System > Configuration > Certificates > Server Certificates > New CSR

☑ Importieren eines signierten Serverzertifikats, das anhand einer Zertifikatssignaturanforderung erstellt wurde

Wenn Sie eine Zertifikatssignaturanforderung über die Webkonsole erstellen, wird auf der Registerkarte **Server Certificate** das Formular **Import the Certificate for a pending CSR** angezeigt.

So importieren Sie ein signiertes Serverzertifikat, das anhand einer Zertifikatssignaturanforderung erstellt wurde:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > Server Certificate** aus.
2. Klicken Sie auf **Import/Renew**.
3. Navigieren Sie unter **Import the Certificate for a pending CSR** zu der Zertifikatdatei, die Sie von der Zertifizierungsstelle erhalten haben, und klicken Sie dann auf **Import** (**Abbildung 23** auf Seite 149).

Registerkarte „Certificates > CA Certificate“

Verwenden Sie die Registerkarte **System > Configuration > Certificates > CA Certificate**, um ein Stammzertifikat zu importieren. Wenn Sie festlegen, dass die Benutzer zur Anmeldung am IVE ein clientseitiges Zertifikat angeben müssen, müssen Sie ein Stammzertifikat angeben. Anhand des Stammzertifikats wird überprüft, ob das vom Browser bereitgestellte Zertifikat gültig ist. Weitere Informationen finden Sie unter „Clientzertifikate“ auf Seite 70.

☑ Importieren eines Stammzertifikats zur Überprüfung clientseitiger Zertifikate

Hinweis: Das IVE unterstützt keine Zwischenserverzertifikate. Wenn Sie ein ***verkettetes Zertifikat*** , d.h. ein vom Schlüssel eines Stammzertifikats signiertes Zwischenzertifikat, in das IVE importieren, importiert das IVE nur das erste Zertifikat. Wenn der Benutzer dann auf das IVE zugreifen möchte, wird eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. (Diese Warnung wird auch angezeigt, wenn der Benutzer ein Stammzertifikat in das IVE importiert, das nicht in den Browser des Benutzers eingebettet ist.) Beachten Sie jedoch, dass das VeriSign-Zwischenzertifikat in das IVE eingebettet ist. Wenn Sie den Stamm eines verketteten VeriSign-Serverzertifikats importieren, wird dem Benutzer daher keine Warnung vor einem nicht vertrauenswürdigen Zertifikat angezeigt.

So geben Sie ein Stammzertifikat an:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > CA Certificate** aus.
2. Klicken Sie auf **Import Certificate**.
3. Navigieren Sie zu der Datei mit dem signierten Zertifikat für das Stammzertifikat, und klicken Sie auf **Import**.

4. Verwenden Sie die Einstellungen auf der Registerkarte **Users > Authentication > Authentication Policy > Certificate**, um das Zertifikat zu aktivieren und optional bestimmte Werte für ausgewählte Zertifikatfelder erforderlich zu machen.
5. Mit den Einstellungen auf der Registerkarte **Users > Authentication > Authentication Policy > Certificate** können Sie Zertifikateinstellungen auf Bereichsebene festlegen.

Wichtig: Wenn Sie keinen Zertifikatserver verwenden, wird die clientseitige SSL-Authentifizierung erst aktiviert, wenn Sie diese Option im Bereich der Seite **Authentication Policy** explizit auswählen.

---

6. Mit den Einstellungen auf der Registerkarte **Users > Roles > General > Restrictions > Certificates** können Sie Zertifikateinstellungen für Rollen festlegen.

Wichtig: Um Zertifikatseinschränkungen für Rollen zu aktivieren, müssen Sie zunächst das Speichern von Zertifikatinformationen aktivieren oder Zertifikateinschränkungen für Bereiche auf der Registerkarte **Users > Authentication > Authentication Policy > Certificate** aktivieren.

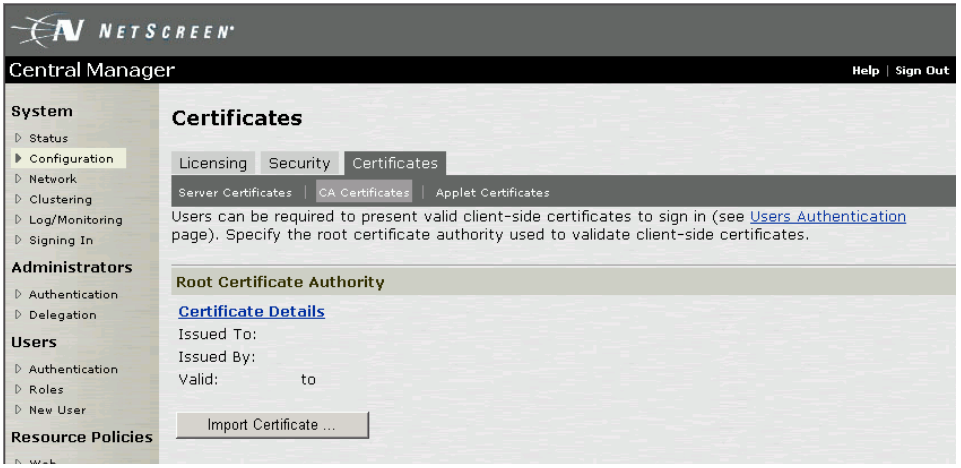


Abbildung 25: System > Configuration > Certificates > CA Certificates

Registerkarte „Certificates > Applet Certificates“

Importieren Sie mithilfe der Registerkarte **System > Configuration > Certificates > Applet Certificate** Codesignaturzertifikate für die Benutzer, wie unter „Appletzertifikate“ auf Seite 71 beschrieben.

☑ Importieren eines Codesignaturzertifikats

So importieren Sie ein Codesignaturzertifikat:

1. Wählen Sie in der Webkonsole **System > Configuration > Certificates > Applet Certificates** aus.
2. Klicken Sie unter **Applet Signing Certificates** auf **Import Certificates**.
3. Navigieren Sie auf der Seite **Import Certificates** zu den entsprechenden Dateien mit dem Codesignaturzertifikat, geben Sie die Informationen für den Kennwortschlüssel ein, und klicken Sie dann auf **Import**.
4. Geben Sie mithilfe der Einstellungen auf der Registerkarte **Resource Policies > Web > Java > Code Signing** an, welche Ressourcen von dem Appletzertifikat erneut signiert werden sollen.

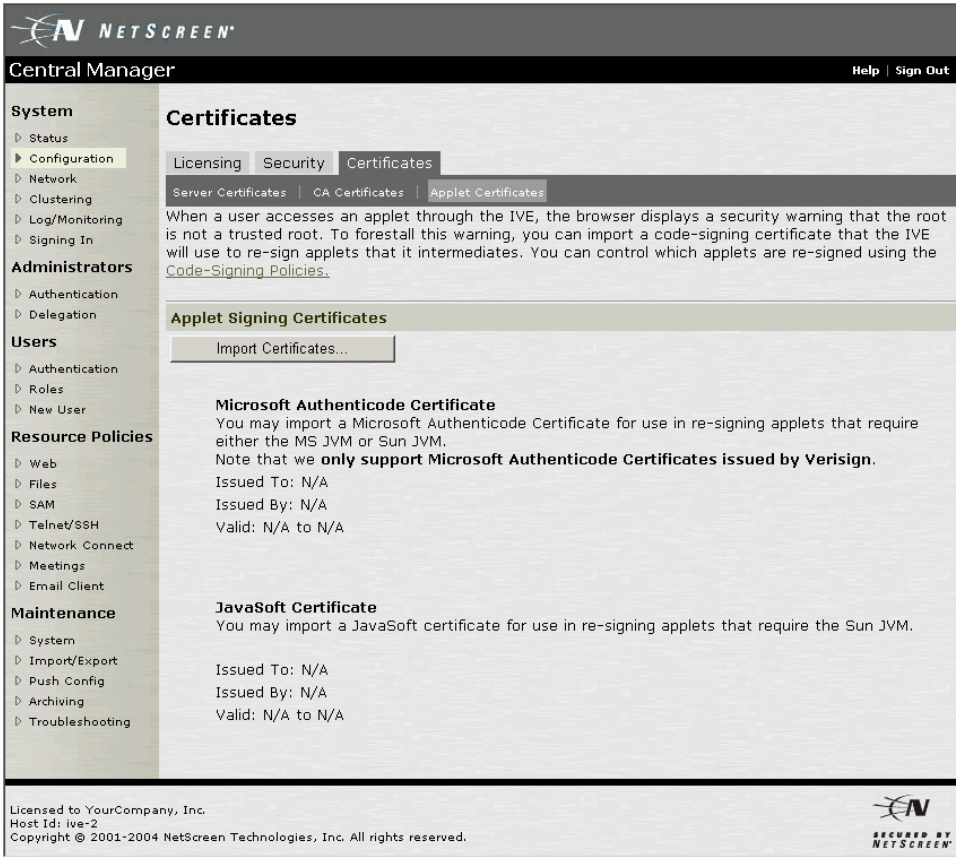


Abbildung 26: System > Configuration > Certificates > Applet Certificates

Konfigurieren der Seite „Network“

Die Seite **System > Network** enthält die folgenden Registerkarten:

Registerkarte „Internal Port“ 157
Registerkarte „External Port“ 161
Registerkarte „Static Routes“ 163
Registerkarte „Hosts“ 164
..... 165

Verwenden Sie die Seite **System > Network** für die folgenden Aufgaben:

Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle) 157
Aktivieren des externen Ports (DMZ-Schnittstelle) 161
Angeben von statischen Routen für den Netzwerkverkehr 163
Angeben von Hostnamen, die vom IVE lokal aufgelöst werden sollen 164

Registerkarte „Internal Port“

Wenn Sie die IVE appliance installieren, nehmen Sie grundlegende Einstellungen für die LAN-Verbindung über den internen Port der Appliance vor. Über den internen Port werden alle WAN- und LAN-Anforderungen an jede Ressource abgewickelt, d.h. Webbrowserabfragen, Dateiabfragen, Authentifizierung und ausgehende Mailanforderungen. Nachdem Sie das IVE eingerichtet haben, können Sie mithilfe der Registerkarte **System > Network > Internal Port** die ursprünglichen Einstellungen bei Bedarf aktualisieren. (Sie können die Appliance auch im Dual-Port-Modus bereitstellen, um eingehende Proxy-SSL-Verbindungen für Web und E-Mail an einem externen Port abzufragen, wie unter „Registerkarte „External Port““ auf Seite 161 beschrieben.) Außerdem können Sie auf der Registerkarte **System > Network > Internal Port** Einstellungen für den zusätzlichen virtuellen Hostnamen, WINS und den Masterbrowser konfigurieren.

☑ Ändern von Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle)

Auf der Registerkarte **Internal Port** können Sie die Netzwerkeinstellungen ändern, die Sie bei der ersten Konfiguration eingegeben haben, und Einstellungen für den zusätzlichen virtuellen Hostnamen, WINS und Masterbrowser konfigurieren.

Hinweis: In den meisten Feldern dieser Seite werden bereits die bei der IVE-Installation eingegebenen Einstellungen angezeigt.

So ändern Sie Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle):

1. Wählen Sie in der Webkonsole **System > Network > Internal Port** aus.
2. Geben Sie im Feld **Virtual Hostname** den vollständig qualifizierten Hostnamen des IVE ein, der von Secure Meeting und den „Pass Through Proxy"-Funktionen verwendet werden soll. Secure Meeting verwendet den angegebenen Hostnamen zum Einfügen der Konferenz-URLs in Benachrichtigungs-E-Mails und für SMTP-Aufrufe(Seite 375). Die Funktion „Pass Through Proxy" verwendet den angegebenen Hostnamen als Alias für den Hostnamen des Anwendungsservers (Seite 348).

   Hinweis: Wenn die IVE-Appliances in einem Cluster gruppiert sind, wird der angegebene virtuelle Hostname im Cluster synchronisiert. In Clustern mit mehreren Sites empfiehlt es sich jedoch, diese Einstellung zu überschreiben und unterschiedliche Hostnamen für die einzelnen Knoten des Clusters mithilfe der Optionen auf der Seite **System > Clustering** anzugeben.
3. Aktualisieren Sie im Abschnitt **Address Information** die Einstellungen für IP-Adresse, Netzmaske, Gateway und Übertragungsrate für die jeweilige IVE-Appliance. Diese Felder enthalten standardmäßig die Einstellungen, die beim ersten IVE-Setup eingegeben wurden.
4. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll. Cluster von IVE-Appliances senden ARP-Anforderungen[1] an die Gateways von anderen IVE-Appliances, um zu überprüfen, ob die Kommunikation ordnungsgemäß erfolgt.

   Wichtig: Wenn Sie das IVE nicht in einer Clusterumgebung ausführen, wird diese Einstellung nicht verwendet. Wenn die IVEs in einem Cluster gruppiert sind, wird die angegebene Höchstdauer im Cluster synchronisiert.
   In Clustern mit mehreren Sites können Sie diese Einstellung für die einzelnen Clusterknoten mithilfe der Optionen auf der Seite **System > Clustering** überschreiben. Seien Sie jedoch vorsichtig, wenn Sie diese Einstellung in Aktiv/Passiv-Clustern ändern, da das IVE auch die Einstellung **ARP Ping Timeout** auf der Registerkarte **Internal** als Failover-Zeitgeber für die VIP verwendet.

1. Das IVE führt beim Versuch, die Kommunikation im Cluster einzurichten, zwei ARP-Anforderungen aus – eine an das Gateway des internen Ports und eine an das Gateway des externen Ports.

5. Aktualisieren Sie im Abschnitt **DNS Name Resolution** die primäre DNS-Adresse, die sekundäre DNS-Adresse und den DNS-Standarddomänennamen für die IVE-Appliance. Sie können in diesen Feldern mehrere DNS-Domänen angeben, das IVE durchsucht sie in der Reihenfolge, in der sie aufgeführt sind.
6. Geben Sie im Feld **WINS** den Namen oder die IP-Adresse für den WINS-Server (Windows Internet Naming Service) ein, mit dem Sie Namen von Arbeitsstationen und Standorten IP-Adressen zuweisen (sofern vorhanden). Sie können einen lokalen oder einen Remote-WINS-Server auswählen.
7. Aktivieren Sie das Kontrollkästchen **Enable Network Discovery**, damit das IVE freigegebene Windows-Ordner erkennen kann.
8. Klicken Sie auf **Master Browsers**, um einen WINS-Server, Domänencontroller oder anderen Server in der IVE-Domäne auszuwählen, der auf die NETBIOS-Aufrufe reagiert und Namen von Arbeitsstationen und Standorten IP-Adressen zuordnet (sofern vorhanden). Fügen Sie den Masterbrowser dann über die Seite **Windows Networking – Specify Master Browser** hinzu.
9. Klicken Sie auf der Registerkarte **Internal Port** auf **Save Changes**.

So setzen Sie Netzwerkeinstellungen für den internen Port (LAN-Schnittstelle) zurück:

1. Wählen Sie in der Webkonsole **System > Network > Internal Port** aus.
2. Klicken Sie auf **Reset**, um auf die letzten gespeicherten Änderungen zurückzusetzen.

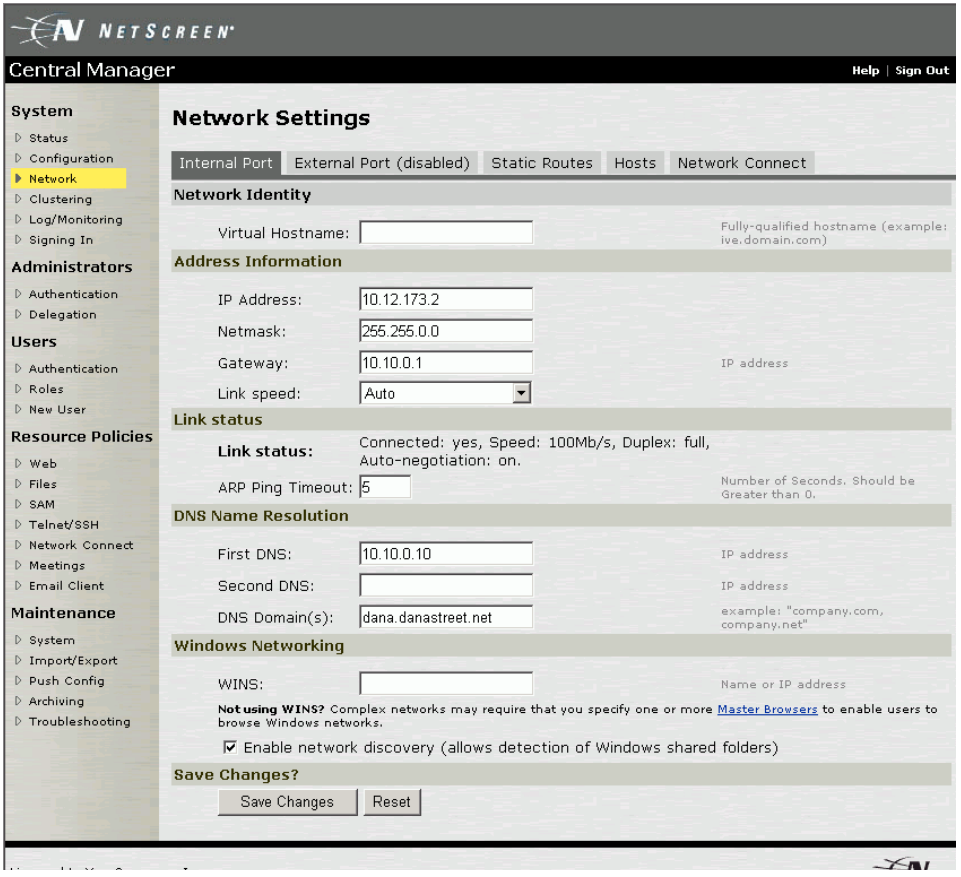


Abbildung 27: System > Network > Internal Port

Registerkarte „External Port“

Die externe DMZ-Schnittstelle (Demilitarized Zone) fragt nur Anforderungen von Benutzern ab, die am IVE angemeldet sind, und leitet nur deren Anforderungen weiter. Vor dem Senden eines Pakets ermittelt das IVE, ob das Paket einer TCP-Verbindung zugeordnet ist, die von einem Benutzer über die externe Schnittstelle initiiert wurde. Ist dies der Fall, sendet das IVE das Paket an die externe Schnittstelle. Alle übrigen Pakete werden an die interne Schnittstelle gesendet. Die für jede Schnittstelle festgelegten Routen werden verwendet, nachdem das IVE ermittelt hat, ob die interne oder die externe Schnittstelle zu verwenden ist. Das IVE leitet keine Anforderungen von der externen Schnittstelle ein, und diese Schnittstelle akzeptiert keine anderen Verbindungen (mit Ausnahme von Ping- und Traceroutеverbindungen). Alle Anforderungen an eine beliebige Ressource werden von der internen Schnittstelle ausgegeben. (Weitere Informationen finden Sie unter „Registerkarte „Internal Port““ auf Seite 157.)

☑ Aktivieren des externen Ports (DMZ-Schnittstelle)

Auf der Registerkarte **External Port** können Sie die DMZ-Funktion aktivieren.

Hinweis: Der externe Port fragt nur Anforderungen von Benutzern ab, die am IVE angemeldet sind, und leitet nur deren Anforderungen weiter. Wenn Sie die DMZ-Funktion aktivieren, können sich Administratoren standardmäßig nicht mehr von einem externen Standort aus anmelden. Sie können den externen Port für Administratoren auf der Registerkarte **Administrators > Authentication > Authentication Policy > Source IP** öffnen.

So aktivieren Sie den externen Port:

1. Wählen Sie in der Webkonsole **System > Network** > **External Port** aus.
2. Wählen Sie unter **DMZ Setting** die Option **Enable** aus.
3. Geben Sie unter **Address Information** IP-Adresse, Netzmaske, Gateway und Übertragungsrate für den externen Port des IVE ein. In den meisten Fällen empfiehlt es sich, die Einstellungen von der Seite **Internal Port** zu übernehmen und dann die Informationen zum internen Port in eine lokale IP-Adresse und Netzmaske sowie ein lokales Gateway zu ändern.
4. Geben Sie im Feld **ARP Ping Timeout** an, wie lange das IVE höchstens auf Antworten auf ARP-Anforderungen (Address Resolution Protocol) warten soll. Cluster von IVE-Appliances senden ARP-Anforderungen[1]an

die Gateways von anderen IVE-Appliances, um zu überprüfen, ob die Kommunikation ordnunggemäß erfolgt.

Hinweis: Wenn die IVEs in einem Cluster gruppiert sind, wird die angegebene Höchstdauer im Cluster synchronisiert. In Clustern mit mehreren Sites können Sie diese Einstellung für die einzelnen Knoten mithilfe der Optionen auf der Seite **System > Clustering** überschreiben. Wenn Sie das IVE nicht in einer Clusterumgebung ausführen, wird die Einstellung für **ARP Ping Timeout** nicht verwendet.

---

5. Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

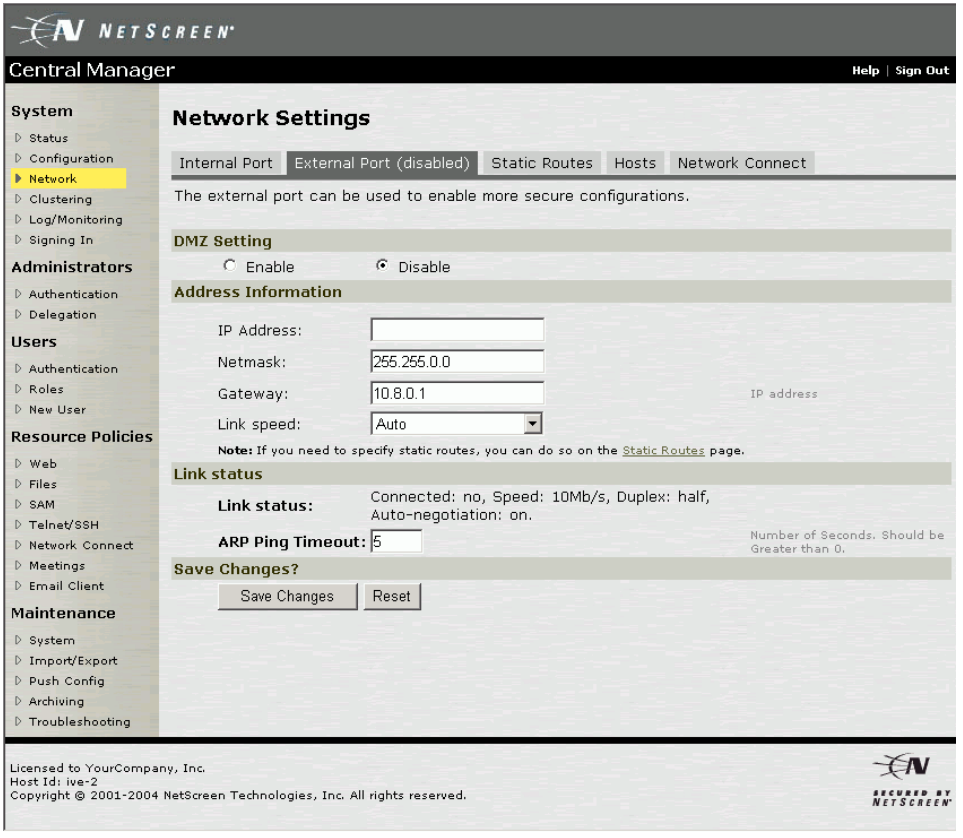


Abbildung 28: System > Network > External Port

1. Das IVE führt beim Versuch, die Kommunikation im Cluster einzurichten, zwei ARP-Anforderungen aus – eine an das Gateway des internen Ports und eine an das Gateway des externen Ports.

Registerkarte „Static Routes“

☑ Angeben von statischen Routen für den Netzwerkverkehr

Auf der Registerkarte **Static Routes** können Sie Routingtabelleneinträge hinzufügen.

Hinweis: Alle Verbindungsanforderungen an interne Ressourcen erfolgen von dem internen IVE-Port aus, unabhängig von den Routeneinstellungen. Die Routeneinstellungen des externen Ports werden nur zur Weiterleitung von Paketen verwendet, die Verbindungen zugeordnet sind, die von einem Remoteclient initiiert wurden. Weitere Informationen finden Sie unter „Registerkarte „External Port““ auf Seite 161.

So geben Sie statische Routen an:

1. Wählen Sie in der Webkonsole **System > Network > Static Routes** aus.
2. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Add**.

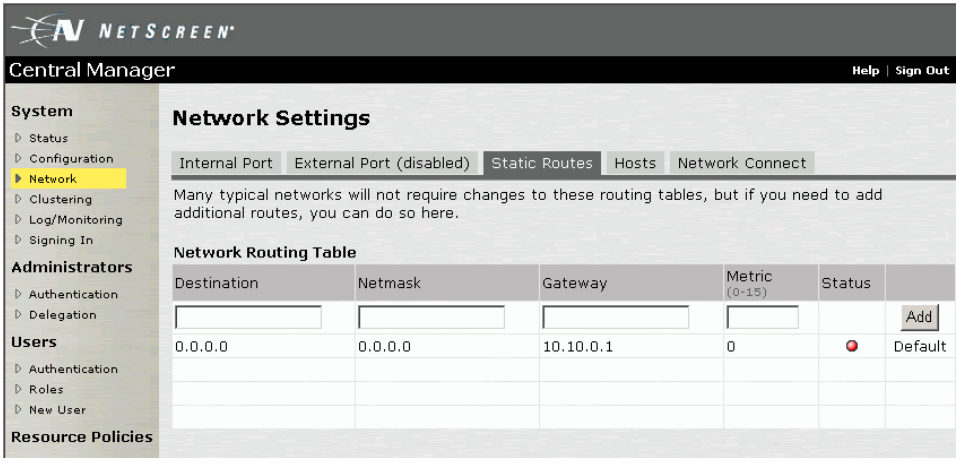


Abbildung 29: **System > Network > Static Routes**

Registerkarte „Hosts“

☑ Angeben von Hostnamen, die vom IVE lokal aufgelöst werden sollen

Auf der Registerkarte **Hosts** können Sie Hostnamen angeben, die vom IVE lokal zu IP-Adressen aufgelöst werden können. Diese Funktion bietet sich in folgenden Fällen an:

- Das IVE kann nicht auf den DNS-Server zugreifen
- Im LAN wird über WINS auf Server zugegriffen
- Die Sicherheitsrichtlinien Ihres Unternehmens lassen die Auflistung interner Server auf einem externen DNS nicht zu oder erfordern die Maskierung interner Hostnamen

Wenn Sie auf der Registerkarte **System > Network Settings > Hosts** eines Clusters Hostnamenzuordnungen eingeben, werden die Einstellungen für die anderen Knoten übernommen. Wenn Sie Zuordnungen von Hostnamen für einen bestimmten Knoten eingeben möchten, wählen Sie die Registerkarte **System > Clustering**, anschließend in der Liste **Cluster Members** einen Knoten und dann für diesen Knoten die Registerkarte **Hosts** aus.

So geben Sie Hostnamen an, die das IVE lokal auflösen soll:

1. Wählen Sie in der Webkonsole die Registerkarte **Network > Network Settings > Hosts** aus.
2. Geben Sie eine IP-Adresse, eine durch Kommas getrennte Liste von Hostnamen, die zu der IP-Adresse aufgelöst werden, und bei Bedarf einen Kommentar von höchstens 200 Wörtern ein, und klicken Sie dann auf **Add**.

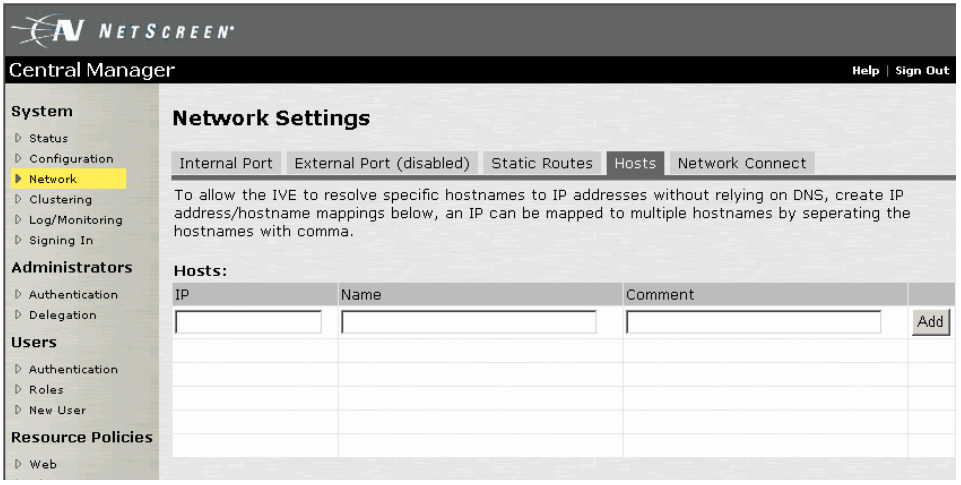


Abbildung 30: System > Network > Hosts

Konfigurieren der Seite „Clustering“

Wir empfehlen, einen Cluster zunächst in einer Stagingumgebung bereitzustellen und erst zu einer Produktionsumgebung zu wechseln, nachdem Sie den Authentifizierungsbereich, die Benutzerrolle und Ressourcenrichtlinie sowie die Anwendungen, die die Endbenutzer möglicherweise verwenden, getestet haben.

Wichtig: Vor dem Erstellen eines Clusters müssen Sie sicherstellen, dass es sich bei allen vorgesehenen IVE-Knoten um die gleiche Hardwareplattform handelt (beispielsweise ausschließlich A3000-Geräte), und dass auf allen Knoten die gleiche Dienstpaketversion ausgeführt wird.

Die Seite **System > Clustering** enthält die folgenden Registerkarten:

Registerkarte „Create“ 168
Registerkarte „Status“ 170
Registrierkarte „Join“ 175
Registerkarte „Properties“ 182

Auf den Registerkarten der Seite **System >Clustering** können Sie Folgendes durchführen:

Definieren und Initialisieren eines Clusters 168
Angeben eines neuen Clustermitglieds 170
Verwalten von Netzwerkeinstellungen für Clusterknoten 172
Aktualisieren des Dienstpakets für Clusterknoten 173
Hinzufügen eines IVE zu einem Cluster über die Webkonsole 176
Hinzufügen eines IVE zu einem Cluster über die serielle Konsole 179
Ändern von Clustereigenschaften oder Löschen eines Clusters 182

Übersichtsinformationen zu Clustern finden Sie unter „Cluster – Übersicht“ auf Seite 75.

Registerkarte „Create“

Beim Erstellen eines Clusterpaares, eines Cluster mit mehreren Einheiten oder eines Clusters mit mehreren Sites werden die Clustereinstellungen zunächst für nur ein IVE festgelegt, und anschließend werden weitere Mitglieder hinzugefügt. Verwenden Sie die Registerkarte **Create**, um einen Cluster zu definieren und initialisieren. Nach Angabe der Clustereinstellungen wird anstelle der Registerkarte **Create** die Registerkarte **Status** angezeigt. Über diese Registerkarte können Sie dem Cluster weitere IVEs hinzufügen und den Cluster verwalten.

☑ Definieren und Initialisieren eines Clusters

Wir empfehlen, vor dem Definieren eines Clusters zunächst die System- und Benutzereinstellungen auf einem IVE zu konfigurieren. Erstellen Sie anschließend auf dem gleichen IVE den Cluster. Dieses IVE wird dem Cluster im Rahmen des Erstellungsvorgangs hinzugefügt. Wenn dem Cluster weitere IVEs beitreten, gibt dieses IVE seine Konfiguration an die neuen Clustermitglieder weiter.

So definieren und initialisieren Sie einen Cluster:

1. Konfigurieren Sie ein IVE mit den gewünschten System-, Benutzer-, Ressourcen- und Anwendungseinstellungen.
2. Wählen Sie in der Webkonsole des konfigurierten IVE die Registerkarte **System > Configuration > Licensing** aus, und geben Sie Ihren Lizenzcode ein, um die Clusterfunktion zu aktivieren. Unter der Überschrift **System** wird die Menüoption **Clustering** angezeigt.
3. Geben Sie auf der Registerkarte **System > Clustering >Create** die Bezeichnung für den Cluster, ein Clusterkennwort und einen Namen für dieses IVE ein, zum Beispiel `ive-1`.

   Hinweis: Wenn Sie weitere IVEs konfigurieren, die dem Cluster hinzugefügt werden sollen, müssen Sie das Kennwort erneut eingeben. Alle IVEs in dem Cluster verwenden dieses Kennwort für die Kommunikation.

4. Klicken Sie auf **Create Cluster**. Klicken Sie auf **Create**, wenn Sie aufgefordert werden, die Erstellung des neuen Clusters zu bestätigen. Nachdem das IVE den Cluster initialisiert hat, werden auf der Seite **Clustering** die Registerkarten **Status** und **Properties** angezeigt.

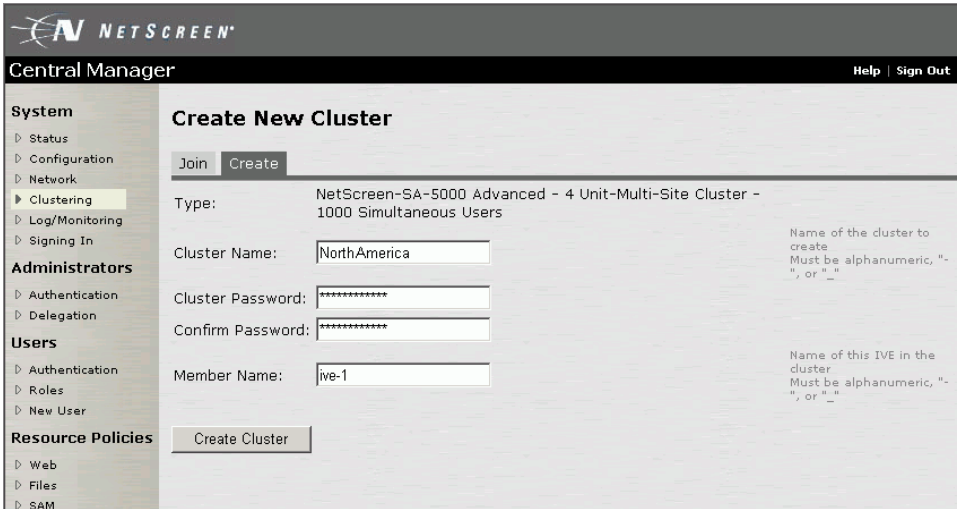


Abbildung 31: System > Clustering: Startseite

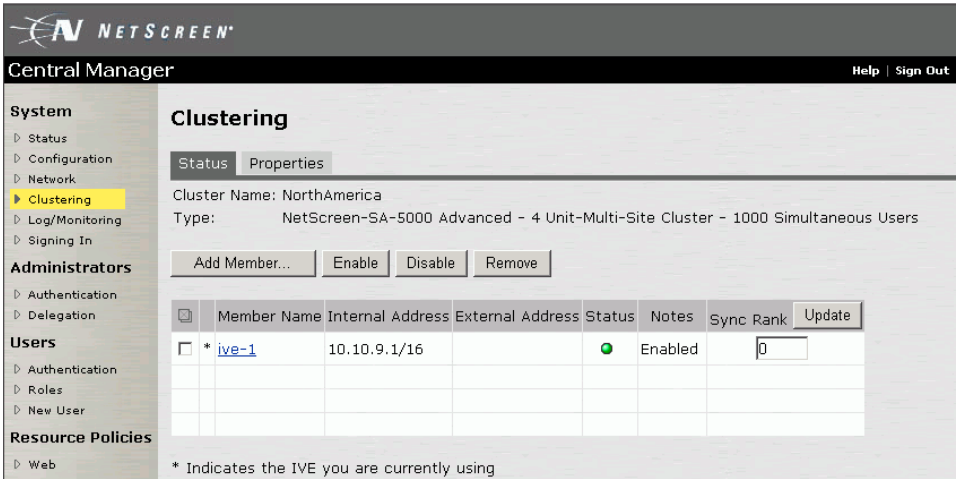


Abbildung 32: System > Clustering: Nach der Definition eines Clusters
Die Abbildung zeigt die Seite „Clustering" nach der Erstellung eines Clusters. Das IVE, auf dem Sie den Cluster definieren, wird zum ersten Clustermitglied.

Registerkarte „Status“

Auf der Registerkarte **Status** können Sie die IVEs angeben, die Sie einem Cluster hinzufügen möchten, den Status der Clusterknoten überwachen, die Netzwerkeinstellungen für einen bestimmten Knoten bearbeiten und Clusterknoten aktivieren, deaktivieren sowie entfernen. In Tabelle 1 auf Seite 173 werden die auf der Registerkarte **Status** angezeigten Informationen sowie die verschiedenen durchführbaren Verwaltungsaufgaben erläutert.

☑ Angeben eines neuen Clustermitglieds

Bevor ein IVE einem Cluster beitreten kann, müssen Sie seine Netzwerkidentität auf einem aktiven Clustermitglied festlegen.

So geben Sie ein IVE an, das einem bestehenden Cluster hinzugefügt werden soll:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Status** aus.
2. Klicken Sie auf **Add Member**, um ein IVE anzugeben, dass dem Cluster beitritt:
   1. Geben Sie die Bezeichnung für das Mitglied ein.
   2. Geben Sie die interne IP-Adresse des Geräts ein.
   3. Geben Sie die externe IP-Adresse des Geräts ein. Beachten Sie, dass das Feld **External IP address** nur angezeigt wird, wenn Sie den externen Port auf der Registerkarte **System > Network Settings > External Port** aktiviert haben.
   4. Klicken Sie auf **Add Node**.
   5. Klicken Sie auf **Add**, wenn Sie aufgefordert werden, das Hinzufügen des neuen Mitglieds zu bestätigen.
   6. Wiederholen Sie dieses Verfahren für jedes Gerät, das Sie hinzufügen möchten.

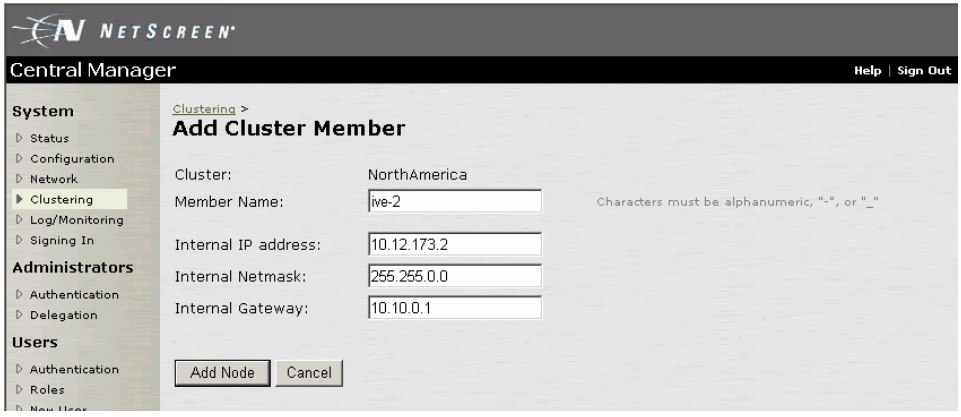


Abbildung 33: System > Clustering > Add Member for a multi-site cluster
Hinweis: Sie können die Felder „Netmask" und „Gateway" nur für Knoten in einem Cluster mit mehreren Sites bearbeiten.

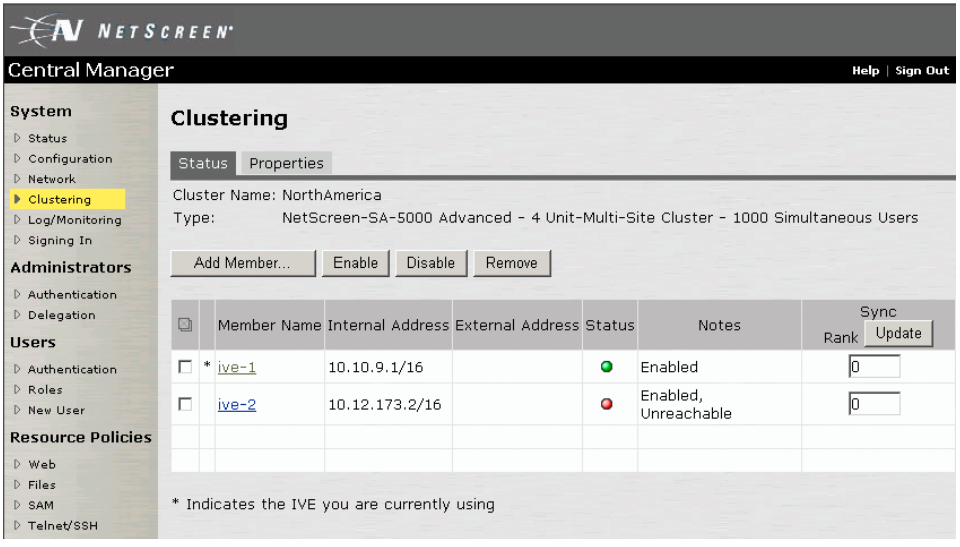


Abbildung 34: System > Clustering > Status: Nach dem Festlegen eines neuen Mitglieds

Wichtige Informationen zum Verwalten von Netzwerkeinstellungen für Knoten in einem Cluster mit mehreren Sites finden Sie unter „Verwalten von Netzwerkeinstellungen für Clusterknoten" auf Seite 172.

☑ Verwalten von Netzwerkeinstellungen für Clusterknoten

Wenn Sie einen Cluster mit mehreren Site betreiben, in dem Knoten in unterschiedlichen Unternetzwerken ausgeführt werden, müssen Sie die knotenspezifischen Informationen über die Registerkarte **System > Clustering > Status** ändern.

So ändern Sie die Netzwerkeinstellungen eines Clusterknotens:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Status** aus.
2. Klicken Sie in der Spalte **Member Name** auf den Namen des Knotens, dessen Netzwerkeinstellungen Sie ändern möchten.

   Für den Clusterknoten wird die Seite **Network Settings** mit den Registerkarten **Clustering**, **Internal Port**, **External Port**, **Static Routes**, **Hosts**, und **Network Connect** (sofern lizenziert) angezeigt. Wenn Sie Änderungen auf diesen Registerkarten speichern, wirken sich die neuen Einstellungen nur auf den entsprechenden Knoten aus.

Wichtig: Wenn Sie die Netzwerkeinstellungen auf der Seite **Network > Network Settings** in der **Webkonsole** eines Clustermitglieds ändern, werden die Änderungen an alle Knoten im Cluster weitergegeben. Um nur die Einstellungen für einen bestimmten Knoten zu ändern, müssen Sie auf der Registerkarte **Status** jedes aktiven Mitglieds eine Verbindung mit der Seite **Network Settings** des Knotens herstellen.

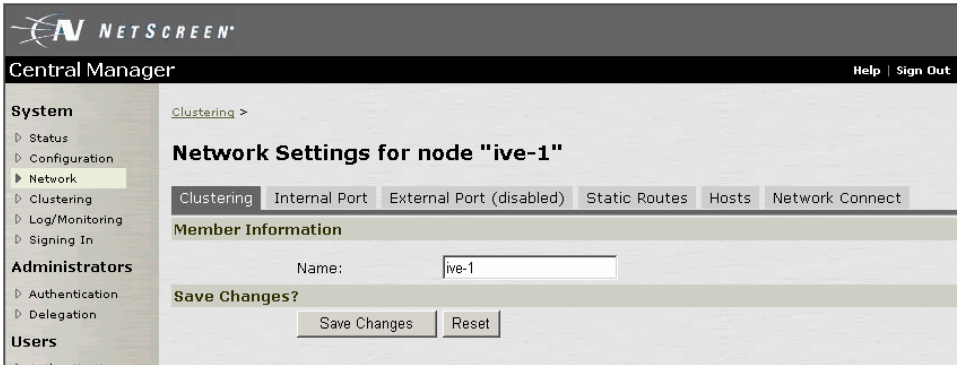


Abbildung 35: System > Clustering > Status: Nach dem Klicken auf einen IVE-Knoten in der Spalte Member Name

Wichtig: Sie können die knotenspezifischen Einstellungen nur über die Registerkarte „Clustering > Status" eines aktiven Mitglieds aufrufen. Das Menü „System > Network" ist hellgrau hervorgehoben. Dies weist Sie darauf hin, dass Sie nicht direkt durch Klicken auf das Netzwerkmenü auf diese Seite gelangt sind, da dieses Menü in dem Fall gelb

hervorgehoben würde. Wenn Sie die Netzwerkeinstellungen für das Cluster auf der Seite „Network Settings" ändern, werden die Änderungen an alle Knoten im Cluster weitergegeben.

☑ Aktualisieren des Dienstpakets für Clusterknoten

Hinweis: Sie können Clustermitglieder nicht herunterstufen. Sie können jedoch jedes Clustermitglied durch ein Rollback auf seinen vorherigen Nicht-Cluster-Zustand zurücksetzen.

So aktualisieren Sie einen Cluster mit einem neueren Dienstpaket:

1. Melden Sie sich bei der **Webkonsole** eines Clusterknotens an.
2. Installieren Sie das Dienstpaket wie unter „Installieren eines NetScreen-Softwaredienstpakets" auf Seite 385 beschrieben.
3. Wenn der Installationsprozess abgeschlossen ist und der Clusterknoten neu startet, weist er die anderen Knoten zur Aktualisierung an.

Tabelle 1: Clustering > Registerkarte „Status"

Element der Benutzeroberfläche	Beschreibung
Schaltfläche **Add Member**	Klicken Sie auf diese Schaltfläche, um ein IVE anzugeben, das dem Cluster beitreten soll. Diesen Schritt müssen Sie für jedes IVE durchführen, das Sie dem Cluster hinzufügen möchten.
Schaltfläche **Enable**	Klicken Sie auf diese Schaltfläche, um einen zuvor deaktivierten Knoten zu aktivieren. Wenn Sie einen Knoten wieder aktivieren, werden alle Statusinformationen auf dem Knoten synchronisiert.
Schaltfläche **Disable**	Klicken Sie auf diese Schaltfläche, um einen Knoten in einem Cluster zu deaktivieren. Der Knoten kommuniziert noch mit dem Cluster, ist jedoch für Statussynchronisierungen deaktiviert und empfängt keine Benutzeranforderungen mehr, es sei denn, der Benutzer meldet sich direkt bei diesem Knoten an.

Tabelle 1: Clustering > Registerkarte „Status“ (Fortsetzung)

Element der Benutzeroberfläche	Beschreibung
Schaltfläche **Remove**	Klicken Sie auf diese Schaltfläche, um den oder die ausgewählten Knoten aus dem Cluster zu entfernen. Nachdem der Knoten entfernt wurde, wird er im eigenständigen Modus ausgeführt.
Spalte **Member Name**	Führt alle Knoten auf, die zu dem Cluster gehören. Sie können auf den Namen eines Knoten klicken, um seinen Namen und die Netzwerkeinstellungen zu ändern.
Spalte **Internal IP Address**	Gibt die interne IP-Adresse des Clustermitglieds in der CIDR-Schreibweise (Classless Inter Domain Routing) an.
Spalte **External IP Address**	Gibt die externe IP-Adresse des Clustermitglieds in der CIDR-Schreibweise (Classless Inter Domain Routing) an. Beachten Sie, dass diese Spalte nur die externe IP-Adresse des Clusterleiters enthält, es sei denn, Sie geben auf seiner eigenen Seite für Netzwerkeinstellungen eine andere Adresse für den Knoten an. Zum Öffnen dieser Seite klicken Sie in der Spalte **Member Name** auf den Namen des Knotens. Wenn Sie die externe IP-Adresse auf der Seite **Network > Network Settings** ändern, wirkt sich die Änderung auf alle Clusterknoten aus.
Spalte **Status**	Gibt den Status des Knotens an: • **Grünes Licht/Enabled** – Der Knoten bearbeitet Benutzeranforderungen und nimmt an der Clustersynchronisierung teil. • **Gelbes Licht/Transitioning** – Der Knoten tritt dem Cluster bei. • **Rotes Licht/Disabled** – Der Knoten bearbeitet keine Benutzeranforderungen und nimmt nicht an der Clustersynchronisierung teil. **Hinweis:** Der Status eines Knotens wird als „eigenständig“ betrachtet, wenn der Knoten außerhalb eines Clusters bereitgestellt wird oder aus einem Cluster entfernt wurde.

Tabelle 1: Clustering > Registerkarte „Status“ (Fortsetzung)

Element der Benutzeroberfläche	Beschreibung
Spalte **Notes**	Gibt den Status der Verbindung des Knotens mit dem Cluster an. Der Status kann folgendermaßen lauten: • OK – Der Knoten ist aktiver Bestandteil des Clusters. • Transitioning – Der Knoten wechselt vom eigenständigen Status in den aktivierten Status. • Unreachable – Der Knoten kommuniziert nicht mehr mit dem Cluster. Ein Clustermitglied kann selbst dann „unreachable“ sein, wenn es online ist und über einen Ping-Befehl erreicht wird. Mögliche Gründe sind: Sein Kennwort ist falsch, es kommuniziert nicht mit allen Clusterknoten, es ist mit einem anderen Gruppenkommunikationsmodus konfiguriert, es führt eine andere Version des Dienstpakets aus oder das IVE ist ausgeschaltet.
Spalte **Sync Rank**	Legt die Reihenfolge fest, in der die Clusterknoten synchronisiert werden sollen. **Hinweis:** Diese Option steht nur mit einer Central Manager-Lizenz zur Verfügung.

Registrierkarte „Join“

Die Art, in der ein IVE einem Cluster beitritt, hängt davon ab, ob es konfiguriert bzw. nicht initialisiert ist. Auf der Registerkarte **Join** können Sie ein konfiguriertes IVE zu einem vorhandenen Cluster hinzufügen. Für ein IVE im Werkzustand empfehlen wir das Verfahren über die serielle Konsole (Seite 179), da für den Beitritt des IVE zum Cluster nur wenige Informationen eingegeben werden müssen.

In einer Access Series FIPS-Umgebung müssen Sie zum Hinzufügen eines IVE zu einem Cluster die **Webkonsole** verwenden. Darüber hinaus müssen Sie über physischen Zugriff auf folgende Einheiten verfügen:

- Die Kryptographiemodule, die an den Frontplatten der IVE-Appliances der Clustermitglieder angebracht sind
- Einen Smartcardleser
- Eine Administratorkarte, die mit der Security World des aktiven Clustermitglieds vorinitialisiert ist

☑ Hinzufügen eines IVE zu einem Cluster über die Webkonsole

Ein werkseitig eingestelltes oder konfiguriertes IVE kann einem Cluster erst hinzugefügt werden, wenn dem Cluster dessen Identität bekannt ist. Anweisungen zur Angabe eines IVE, dass einem Cluster hinzugefügt werden soll, finden Sie unter „Angeben eines neuen Clustermitglieds“ auf Seite 170.

Wichtig: Wenn Sie ein eigenständiges IVE über die **Webkonsole** zu einem Cluster hinzufügen möchten, muss dieses über die gleiche Lizenz verfügen wie die anderen Mitglieder. Außerdem muss das gleiche Dienstpaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

So fügen Sie ein IVE über die Webkonsole einem Cluster hinzu:

1. Wählen Sie in der **Webkonsole** eines bestehenden Clustermitglieds die Registerkarte **System > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „Angeben eines neuen Clustermitglieds“ auf Seite 170.
2. Verfahren Sie folgendermaßen in der **Webkonsole** des IVE, das einem Cluster hinzugefügt werden soll:
   1. Wählen Sie die Registerkarte **System > Configuration > Licensing** aus, und geben Sie den Lizenzcode ein, um die Clusterfunktion zu aktivieren.
   2. Wählen Sie die Registerkarte **System > Clustering > Join** aus, und geben Sie Folgendes ein:
      - Die Bezeichnung des Clusters, dem das IVE beitreten soll
      - Das Clusterkennwort, das Sie beim Definieren des Clusters angegeben haben
      - Die IP-Adresse eines aktiven Clustermitglieds
3. Klicken Sie auf **Join Cluster**. Klicken Sie auf **Join**, wenn Sie aufgefordert werden, den Beitritt zum Cluster zu bestätigen. Nachdem das IVE dem Cluster beigetreten ist, müssen Sie sich erneut anmelden.
4. (Nur Access Series FIPS) Initialisieren Sie den Knoten mit der Security World des aktiven Clustermitglieds. Befolgen Sie dazu die folgenden Anweisungen.

So initialisieren Sie die Security World des Clustermitglieds über die serielle Konsole:

1. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
2. Legen Sie eine Administratorkarte, die mit der Security World des aktiven Clustermitglieds vorinitialisiert wurde, mit den Kontakten nach oben in den Smartcardleser ein.
3. Stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), sofern dieser sich nicht bereits in dieser Position befindet.
4. Stellen Sie eine Verbindung mit der seriellen Konsole des IVE her. Weitere Informationen finden Sie unter „Anhang D: " auf Seite 453.
5. Schalten Sie das IVE aus und dann wieder ein, und überwachen Sie beim Neustart die serielle Konsole. Nach dem Start der Systemsoftware werden Sie in einer Meldung darüber informiert, dass das Gerät als eigenständiges IVE gestartet wird und dass Sie die **TAB-Taste** drücken müssen, um die Clusteroptionen anzuzeigen. Drücken Sie die **TAB-Taste**, wenn Ihnen diese Meldung angezeigt wird.

   Hinweis: Sie müssen die **TAB-Taste** innerhalb von 5 Sekunden drücken. Wenn das Gerät bereits im eigenständigen Modus bootet, warten Sie, bis der Bootvorgang beendet ist, und starten Sie das Gerät dann neu.

6. Geben Sie die Nummer für den Beitritt zu dem bestehenden Cluster ein.
7. Geben Sie die angeforderten Initialisierungsinformationen ein.

Hinweis: Nachdem Sie die Mitglieder eines Access Series FIPS-Clusters mit derselben Security World initialisiert haben, können Sie den Cluster über die **Webkonsole** deaktivieren und wieder aktivieren. Sie müssen nicht mehr die serielle Konsole verwenden, wenn die Clustermitglieder alle Mitglieder derselben Security World sind.

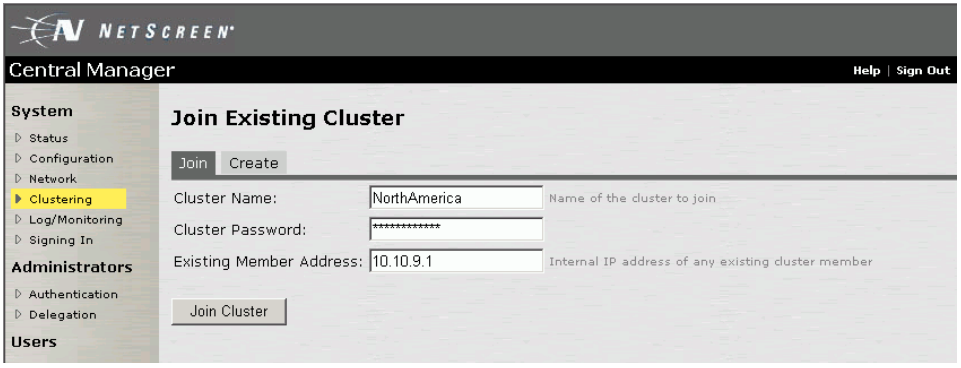


Abbildung 36: System > Clustering > Join: Beitreten zu einem Cluster

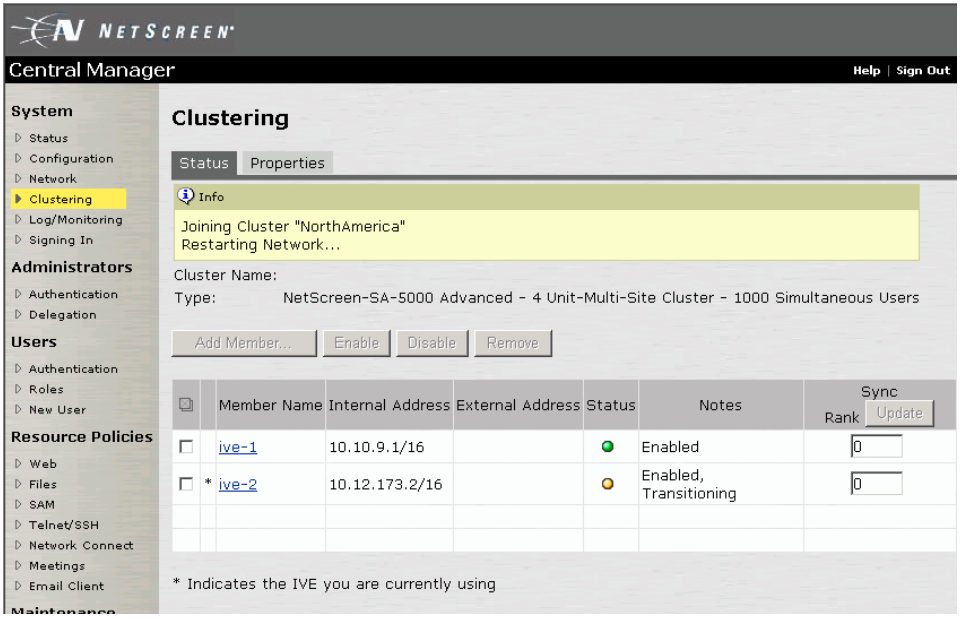


Abbildung 37: System > Clustering > Status: Neustarten von Diensten auf einem neuen Clustermitglied

Sobald ein neuer Knoten eine Verbindung mit einem Cluster herstellt, werden auf der Clusterseite die Registerkarten „Status“ und „Eigenschaften“ angezeigt. Während der neue Knoten seinen Status mit dem aktivierten Clustermitglied synchronisiert, wird sein Status als „Transitioning“ angezeigt.

Verfahren über die serielle Konsole

Sie können ein IVE über seine serielle Konsole zu einem Cluster hinzufügen, es sei denn, diese wird in einer Access Series FIPS-Umgebung ausgeführt. In letzterem Fall müssen Sie jedes IVE über seine Webkonsole hinzufügen. Wenn Sie ein werkseitig eingestelltes IVE zu einem Cluster hinzufügen, empfiehlt es sich, die serielle Konsole zu verwenden. Der Beitritt zu einem bestehenden Cluster kann dann im Verlauf des Initialisierungsvorgangs unter Eingabe nur weniger Informationen erfolgen. Wenn ein IVE einem Cluster beitritt, empfängt es die Clusterstatuseinstellungen. Dabei werden *alle* Einstellungen auf einem IVE mit einer bestehenden Konfiguration überschrieben, und neuen Geräten werden die erforderlichen Vorabinformationen bereitgestellt.

☑ Hinzufügen eines IVE zu einem Cluster über die serielle Konsole

Ein werkseitig eingestelltes oder konfiguriertes IVE kann einem Cluster erst hinzugefügt werden, wenn dem Cluster dessen Identität bekannt ist. Anweisungen zur Angabe eines IVE, dass einem Cluster hinzugefügt werden soll, finden Sie unter „Angeben eines neuen Clustermitglieds“ auf Seite 170.

Wichtig: Wenn Sie ein eigenständiges IVE über die **Webkonsole** zu einem Cluster hinzufügen möchten, muss dieses über die gleiche Lizenz verfügen wie die anderen Mitglieder. Außerdem muss das gleiche Dienstpaket auf der gleichen Hardwareplattform wie bei den anderen Mitgliedern ausgeführt werden.

So fügen Sie ein IVE über seine serielle Konsole zu einem Cluster hinzu:

1. Wählen Sie in der **Webkonsole** eines bestehenden Clustermitglieds die Registerkarte **System > Clustering > Status** aus, und geben Sie das IVE an, das dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „Angeben eines neuen Clustermitglieds“ auf Seite 170.
2. Stellen Sie eine Verbindung mit der seriellen Konsole des IVE her, dass dem Cluster hinzugefügt werden soll. Weitere Informationen finden Sie unter „Anhang D: “ auf Seite 453.
3. Schalten Sie das IVE aus und dann wieder ein, und überwachen Sie beim Neustart die serielle Konsole. Nach dem Start der Systemsoftware werden Sie in einer Meldung informiert, dass das Gerät als eigenständiges IVE gestartet wird und dass Sie die **TAB-Taste** drücken

müssen, um die Clusteroptionen anzuzeigen. Drücken Sie die **TAB-Taste**, wenn Ihnen diese Meldung angezeigt wird.

Hinweis: Sie müssen die **TAB-Taste** innerhalb von 5 Sekunden drücken. Wenn das Gerät bereits im eigenständigen Modus bootet, warten Sie, bis der Bootvorgang beendet ist, und starten Sie das Gerät dann neu.

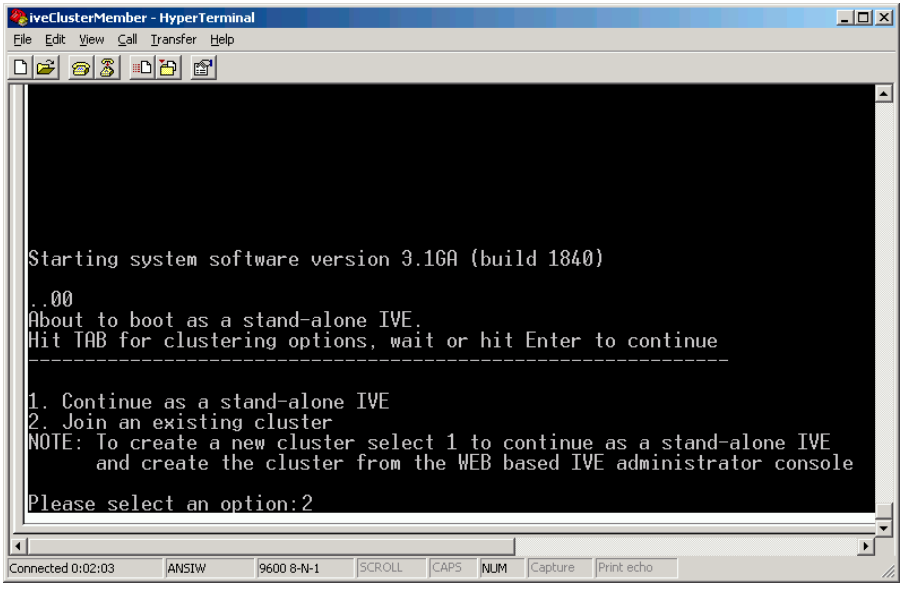

iveClusterMember - HyperTerminal
File Edit View Call Transfer Help
Starting system software version 3.1GA (build 1840)
..00
About to boot as a stand-alone IVE.
Hit TAB for clustering options, wait or hit Enter to continue
1. Continue as a stand-alone IVE
2. Join an existing cluster
NOTE: To create a new cluster select 1 to continue as a stand-alone IVE
and create the cluster from the WEB based IVE administrator console
Please select an option:2
Connected 0:02:03
ANSIW
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Abbildung 38: Serielle Konsole: Clusterbeitrittsoption

4. Geben Sie die Nummer für den Beitritt zu einem bestehenden Cluster ein.
5. Geben Sie die erforderlichen Informationen ein. Dies sind:
   - Die interne IP-Adresse eines aktiven Clustermitglieds.
   - Das Clusterkennwort, d.h. das Kennwort, dass Sie beim Definieren des Clusters eingegeben haben.
   - Der Name des Geräts, das Sie hinzufügen möchten. In diesem Beispiel lautet der Name `ive-2`.
   - Die interne IP-Adresse des Geräts, das Sie hinzufügen möchten.
   - Die Netzmaske des Geräts, das Sie hinzufügen möchten.
   - Das Gateway des Geräts, das Sie hinzufügen möchten.

   Das aktive Clustermitglied überprüft das Clusterkennwort und ob der Name und die IP-Adresse des neuen Geräts mit den Angaben auf der Seite **System > Clustering > Add Cluster Member** in der Webkonsole übereinstimmen. Wenn die Anmeldeinformationen gültig sind, kopiert

das aktive Mitglied alle Statusdaten auf das neue Clustermitglied, einschließlich Lizenz-, Zertifikats-, Benutzer- und Systemdaten.

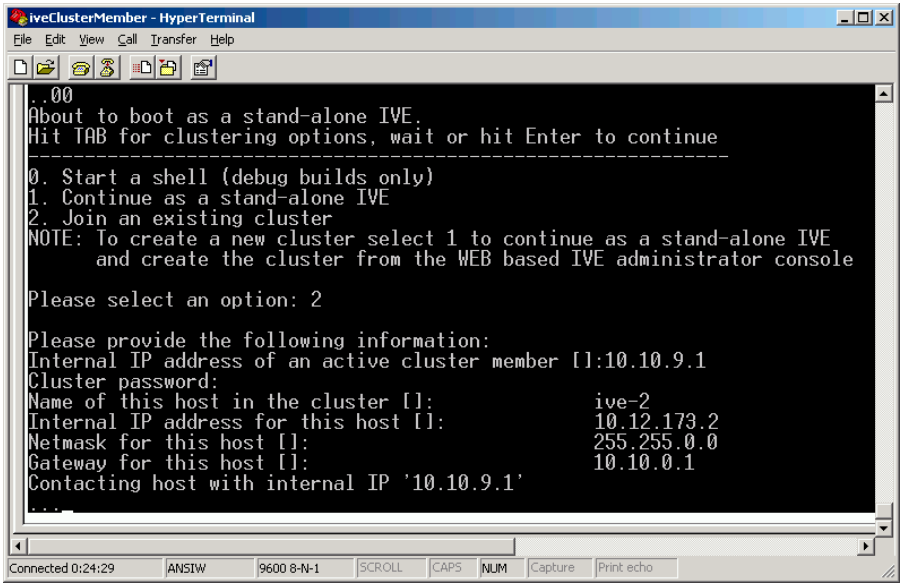

iveClusterMember - HyperTerminal
File Edit View Call Transfer Help
..00
About to boot as a stand-alone IVE.
Hit TAB for clustering options, wait or hit Enter to continue
0. Start a shell (debug builds only)
1. Continue as a stand-alone IVE
2. Join an existing cluster
NOTE: To create a new cluster select 1 to continue as a stand-alone IVE
and create the cluster from the WEB based IVE administrator console
Please select an option: 2
Please provide the following information:
Internal IP address of an active cluster member []:10.10.9.1
Cluster password:
Name of this host in the cluster []: ive-2
Internal IP address for this host []: 10.12.173.2
Netmask for this host []: 255.255.0.0
Gateway for this host []: 10.10.0.1
Contacting host with internal IP '10.10.9.1'
Connected 0:24:29 ANSIW 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Abbildung 39: Serielle Konsole: Angeben des neuen Clustermitglieds

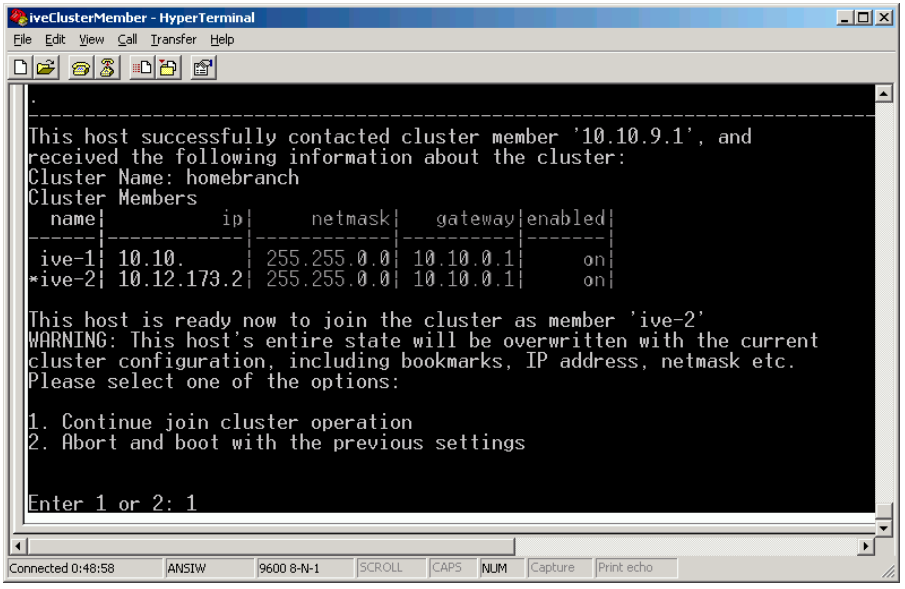

iveClusterMember - HyperTerminal
File Edit View Call Transfer Help
This host successfully contacted cluster member '10.10.9.1', and
received the following information about the cluster:
Cluster Name: homebranch
Cluster Members
name ip netmask gateway enabled
ive-1 10.10. 255.255.0.0 10.10.0.1 on
*ive-2 10.12.173.2 255.255.0.0 10.10.0.1 on
This host is ready now to join the cluster as member 'ive-2'
WARNING: This host's entire state will be overwritten with the current
cluster configuration, including bookmarks, IP address, netmask etc.
Please select one of the options:
1. Continue join cluster operation
2. Abort and boot with the previous settings
Enter 1 or 2: 1
Connected 0:48:58
ANSIW
9600 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Abbildung 40: Serielle Konsole: Bestätigen des Clusterbeitritts

6. Geben Sie zum Fortfahren die Nummer ein. Wenn die Bestätigungsmeldung für den Beitritt des IVE zum Cluster angezeigt wird, überprüfen Sie auf der Registerkarte **Status > Clustering > Status** von allen aktiven Clustermitgliedern, ob der **Status** des neuen Mitglieds als grünes Licht angezeigt wird, d. h., dass das IVE ein aktiver Knoten des Clusters ist.

Registerkarte „Properties“

☑ Ändern von Clustereigenschaften oder Löschen eines Clusters

Auf der Registerkarte **Properties** können Sie den Namen eines Clusters ändern, den Ausführungsmodus eines Clusterpaars angeben, Synchronisierungseinstellungen festlegen oder einen Cluster löschen.

So ändern Sie Clustereigenschaften:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Status** aus.

2. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Save Changes**.
   - Die Clusterbezeichnung können Sie im Feld **Cluster Name** ändern.
   - Um die Konfigurationseinstellung für ein Clusterpaar festzulegen, wählen Sie „Active/Passive" oder „Active/Active" aus. Für eine Aktiv/Passiv-Konfiguration geben Sie eine interne VIP (virtuelle IP-Adresse) und, sofern der externe Port aktiviert ist, eine externe VIP an.

     Hinweis: Der Abschnitt **Configuration Settings** wird nur für Clusterpaare, nicht jedoch für Cluster mit mehreren Einheiten angezeigt.

   - Wählen Sie die gewünschten Synchronisierungseinstellungen aus. Geben Sie dabei auch das zu verwendende Synchronisierungsprotokoll an, und legen Sie fest, ob Protokollmeldungen und Sitzungsdaten der Benutzer synchronisiert werden sollen. Erläuterungen der Synchronisierungseinstellungen finden Sie unter „Statussynchronisierung" auf Seite 79.

- Legen Sie die entsprechenden Überprüfungseinstellungen („Health Check“) für das Netzwerk fest, einschließlich der zulässigen Anzahl von ARP-Pingfehlern, bevor die interne Schnittstelle des IVE deaktiviert wird. Legen Sie auch fest, ob die externe Schnittstelle des IVE bei einem Ausfall der internen Schnittstelle deaktiviert werden soll.

So löschen Sie einen Cluster:

1. Wählen Sie in der **Webkonsole** eines aktiven Clustermitglieds die Registerkarte **System > Clustering > Properties** aus.
2. Wählen Sie **Delete Cluster** aus. Nach Beendigung des Vorgangs werden alle Clusterknoten als eigenständige IVEs ausgeführt.

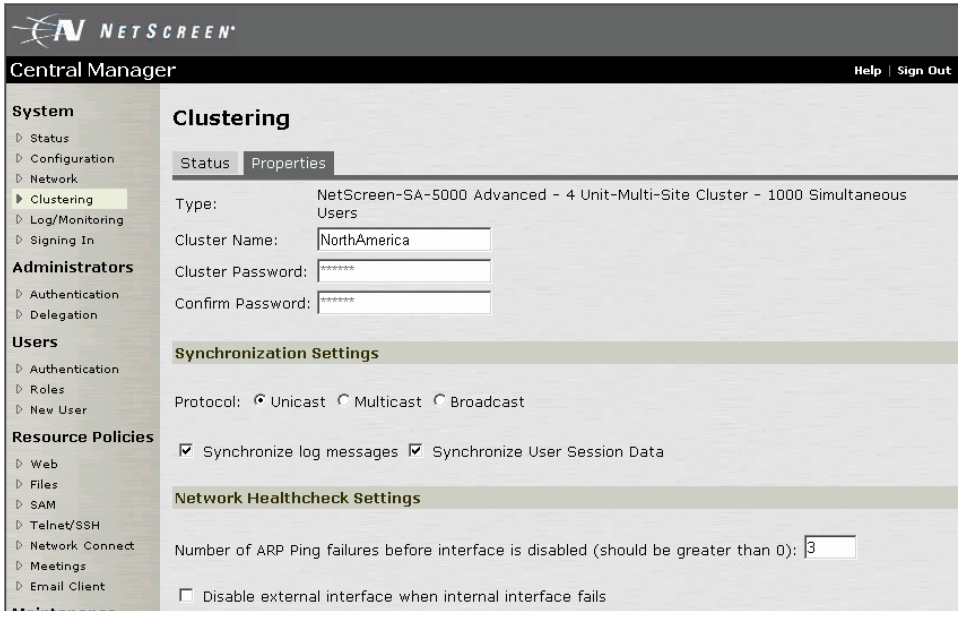


Abbildung 41: System > Clustering > Properties (Cluster mit mehreren Sites)

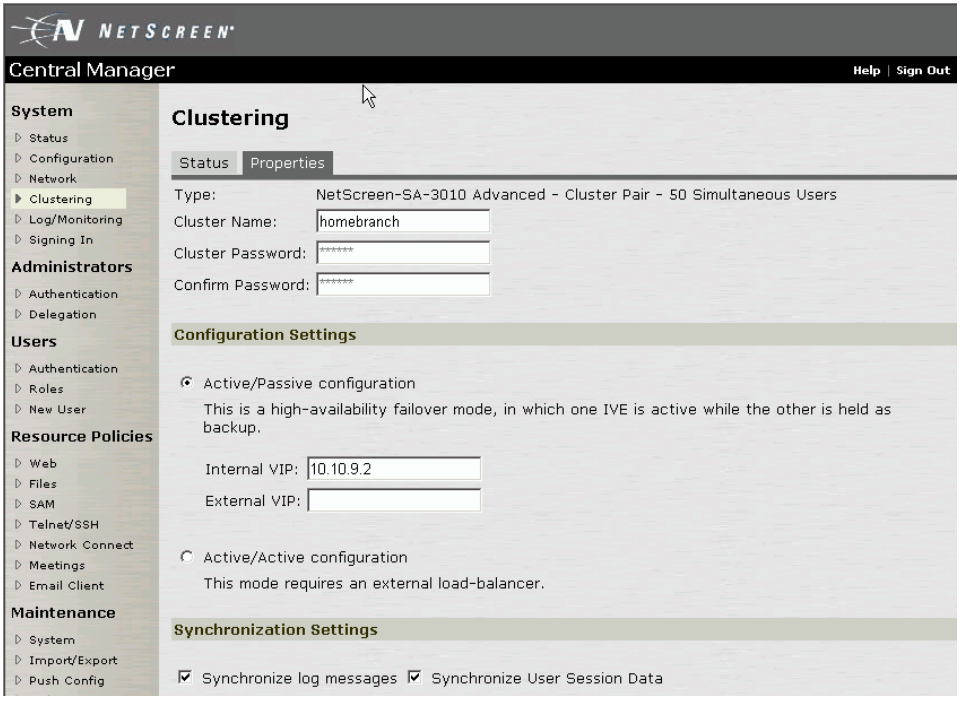


Abbildung 42: System > Clustering > Properties (Clusterpaar)

Konfigurieren der Seite „Log Monitoring“

Die Seite **System > Log Monitoring** enthält die folgenden Registerkarten:

Registerkarten „Events“, „User Access“ und „Admin Access“ 187
Registerkarte „SNMP“ 195
Registerkarte „Statistics“ 200

Auf der Seite **System > Log Monitoring** können Sie Folgendes durchführen:

Speichern, Anzeigen oder Löschen der Protokolldatei 188
Geben Sie an, welche Ereignisse in der Protokolldatei gespeichert werden sollen 189
Erstellen von benutzerdefinierten Filtern und Formaten für Protokolldateien 194
Überwachen des IVE als SNMP-Agent 195
Anzeigen der Systemstatistik 200

Weitere Informationen zu Protokollen und Überwachungsfunktionen des IVE finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 95.

Registerkarten „Events“, „User Access“ und „Admin Access“

Auf den Seiten **System > Log/Monitoring > Events**, **User Access** und **Admin Access** können Sie das Ereignisprotokoll (das die Systemereignisse enthält), das Benutzerzugriffsprotokoll (das die Endbenutzeranforderungen und -änderungen enthält) und das Administratorzugriffsprotokoll (das die Administratoränderungen enthält) filtern und formatieren.

Die Seiten **Events**, **User Access** und **Admin Access** enthalten jeweils die folgenden Registerkarten:

Registerkarte „Log“ 188
Registerkarte „Einstellungen“ 189
Registerkarte „Filters“ 194

Hinweis: Bei den Ereignis-, Benutzerzugriffs- und Administratorzugriffsprotokollen handelt es sich um drei eigenständige Dateien. Obwohl die grundlegenden Konfigurationsanweisungen für alle drei gleich sind, wirken sich Einstellungsänderungen bei einer der Dateien nicht auf die Einstellungen der anderen aus. Weitere Informationen zu den Inhalten der einzelnen Dateien finden Sie unter „Protokollierung und Überwachung – Übersicht“ auf Seite 95.

Registerkarte „Log“

☑ Speichern, Anzeigen oder Löschen der Protokolldatei

So zeigen Sie die Ereignisprotokolldatei an, speichern sie oder löschen sie:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Log** aus.
3. (Gilt nur für Central Manager) Wählen Sie aus der Liste **View by filter** den benutzerdefinierten Filter aus, den das IVE zum Filtern von Daten verwenden sollte.
4. Geben Sie im Feld **Show** eine Nummer ein, und klicken Sie auf **Update**, wenn Sie die Anzahl der jeweils vom IVE angezeigten Protokolleinträge ändern möchten.
5. Klicken Sie auf **Save Log As**, wechseln Sie zum gewünschten Netzwerkspeicherort, geben Sie einen Dateinamen ein, und klicken Sie dann auf **Save**, um die Protokolldatei manuell zu speichern.
6. Klicken Sie auf **Clear Log**, um das lokale Protokoll und die Datei `log.old` zu löschen.

Hinweis: Wenn Sie das lokale Protokoll löschen, wirkt sich dies nicht auf die vom Syslog-Server aufgezeichneten Ereignisse aus. Die nachfolgenden Ereignisse werden in einer neuen lokalen Protokolldatei aufgezeichnet.

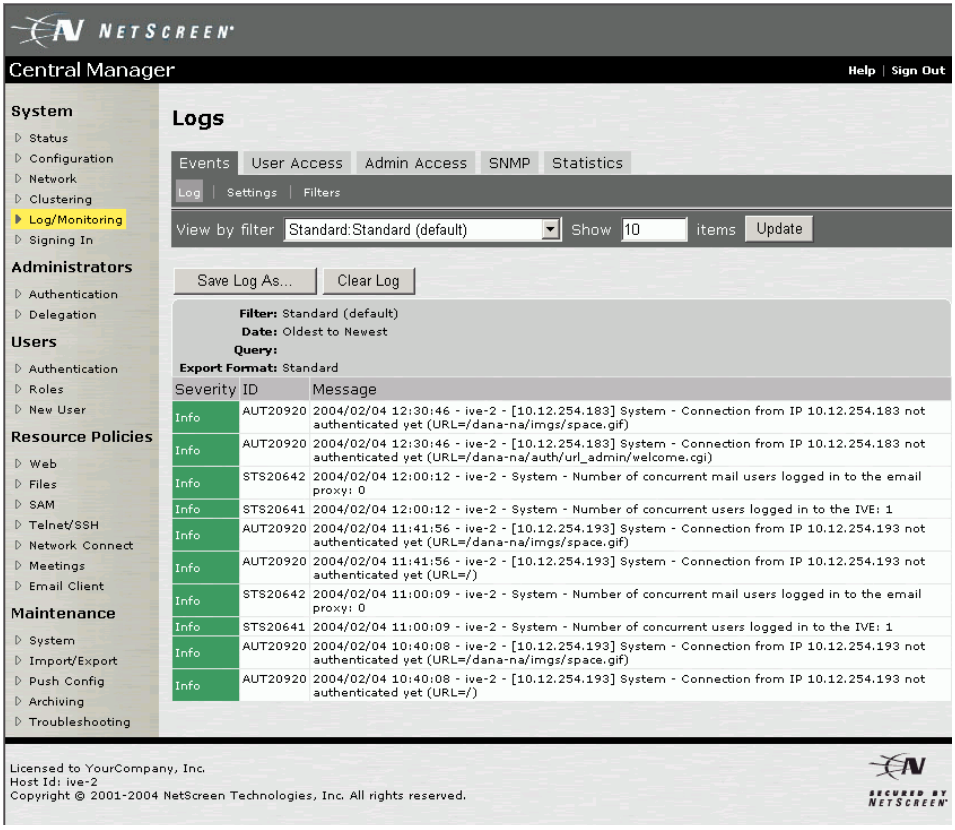

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Logs
Events
User Access
Admin Access
SNMP
Statistics
Log
Settings
Filters
View by filter
Standard:Standard (default)
Show
10
items
Update
Save Log As...
Clear Log
Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard
Severity
ID
Message
Info AUT20920 2004/02/04 12:30:46 - ive-2 - [10.12.254.183] System - Connection from IP 10.12.254.183 not authenticated yet (URL=/dana-na/imgs/space.gif)
Info AUT20920 2004/02/04 12:30:46 - ive-2 - [10.12.254.183] System - Connection from IP 10.12.254.183 not authenticated yet (URL=/dana-na/auth/url_admin/welcome.cgi)
Info STS20642 2004/02/04 12:00:12 - ive-2 - System - Number of concurrent mail users logged in to the email proxy: 0
Info STS20641 2004/02/04 12:00:12 - ive-2 - System - Number of concurrent users logged in to the IVE: 1
Info AUT20920 2004/02/04 11:41:56 - ive-2 - [10.12.254.193] System - Connection from IP 10.12.254.193 not authenticated yet (URL=/dana-na/imgs/space.gif)
Info AUT20920 2004/02/04 11:41:56 - ive-2 - [10.12.254.193] System - Connection from IP 10.12.254.193 not authenticated yet (URL=/)
Info STS20642 2004/02/04 11:00:09 - ive-2 - System - Number of concurrent mail users logged in to the email proxy: 0
Info STS20641 2004/02/04 11:00:09 - ive-2 - System - Number of concurrent users logged in to the IVE: 1
Info AUT20920 2004/02/04 10:40:08 - ive-2 - [10.12.254.193] System - Connection from IP 10.12.254.193 not authenticated yet (URL=/dana-na/imgs/space.gif)
Info AUT20920 2004/02/04 10:40:08 - ive-2 - [10.12.254.193] System - Connection from IP 10.12.254.193 not authenticated yet (URL=/)
Licensed to YourCompany, Inc.
Host Id: ive-2
Copyright © 2001-2004 NetScreen Technologies, Inc. All rights reserved.
SECURED BY NETSCREEN

Abbildung 43: System > Log/Monitoring > Events > Log

Registerkarte „Einstellungen“

☑ Geben Sie an, welche Ereignisse in der Protokolldatei gespeichert werden sollen

Mithilfe der Optionen auf der Registerkarte **Settings** können Sie neben der Höchstdateigröße angeben, was das IVE in die Protokolldatei schreiben und welcher Syslog-Server zum Speichern der Protokolldateien verwendet werden soll.

Hinweis: Sie können auch die Seite **Archiving** verwenden, um die Protokolle automatisch an einem für FTP zugänglichen Ort zu speichern. Weitere Informationen finden Sie unter „Konfigurieren der Seite „Archiving““ auf Seite 403.

So legen Sie die Einstellungen für das Ereignisprotokoll fest:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Settings** aus.
3. Geben Sie in der Liste **Max Log Size** die Höchstdateigröße für die lokale Protokolldatei an. (Die Grenze liegt bei 500 MB.) Im Systemprotokoll werden Daten bis zu der angegebenen Menge angezeigt.

   Hinweis: Max Log Size ist eine interne Einstellung, die weitgehend der Größe von Protokollen entspricht, die mit **Standard** formatiert werden. Wenn Sie ein ausführlicheres Format, wie z.B. **WELF** auswählen, kann die Protokolldatei die hier angegebene Größe überschreiten.

4. Aktivieren Sie unter **Select Events to Log** die Kontrollkästchen für die einzelnen Ereignisarten, die in der lokalen Protokolldatei erfasst werden sollen.

   Hinweis: Wenn Sie das Kontrollkästchen **Statistics** auf der Registerkarte **Events** deaktivieren, schreibt das IVE die Statistiken nicht in die Protokolldatei, sondern zeigt sie weiterhin auf der Registerkarte **System > Log/Monitoring > Statistics** an (Seite 200).

5. Geben Sie unter **Syslog Servers** Informationen über den Syslog-Server ein, auf dem die Protokolldateien gespeichert werden sollen (optional):
   1. Geben Sie den Namen oder die IP-Adresse des Syslog-Servers ein.
   2. Geben Sie einen Syslog-Typ („Facility") für den Server ein. Das IVE stellt 8 Facilitys (LOCAL0-LOCAL7) bereit, die Sie den Facilitys auf dem Syslog-Server zuordnen können.
   3. (Gilt nur für Central Manager) Wählen Sie den Filter, den Sie auf die Protokolldatei anwenden möchten.
   4. Klicken Sie auf **Add**.
   5. Wiederholen Sie den Vorgang ggf. für mehrere Server, und verwenden Sie unterschiedliche Formate und Filter für verschiedene Server und Facilitys.

   Wichtig: Vergewissern Sie sich, dass der Syslog-Server Nachrichten mit den folgenden Einstellungen akzeptiert: `facility = LOG_USER` und `level = LOG_INFO`.

6. Klicken Sie auf **Save Changes**.

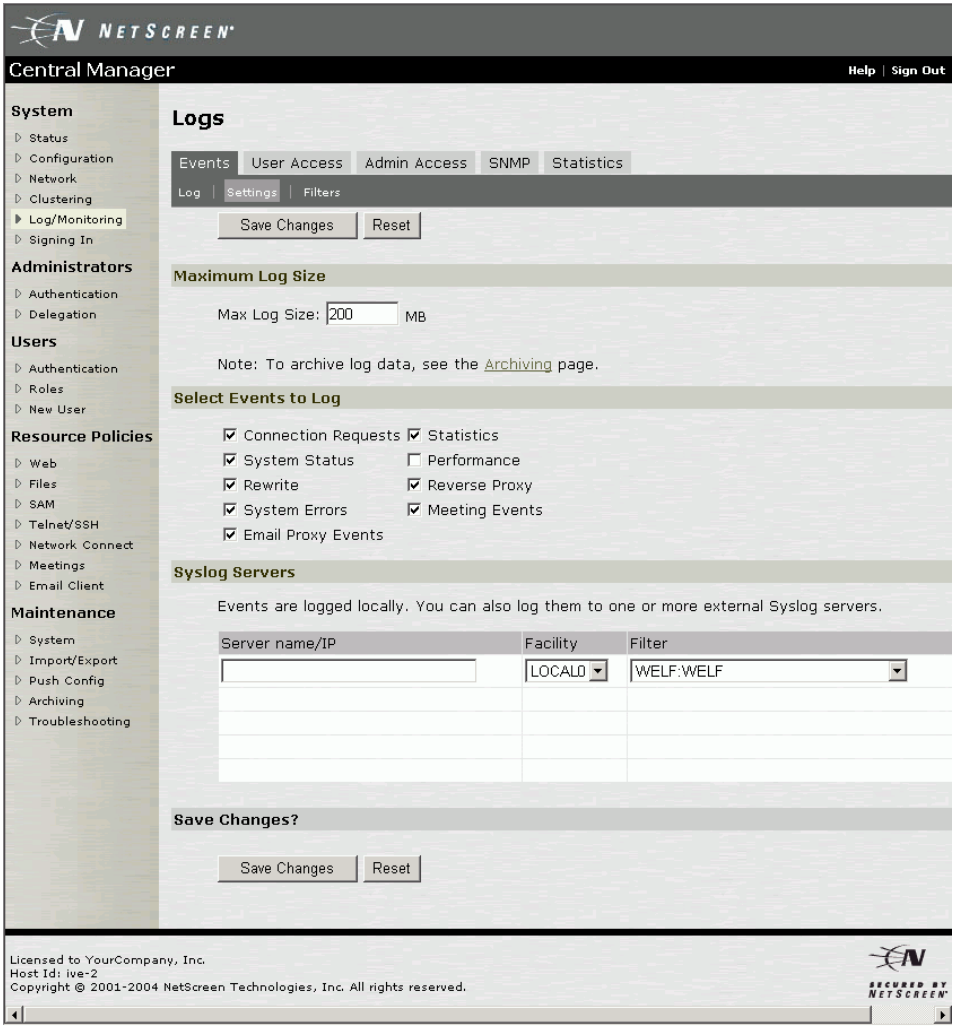


Abbildung 44: System > Log/Monitoring > Events > Settings

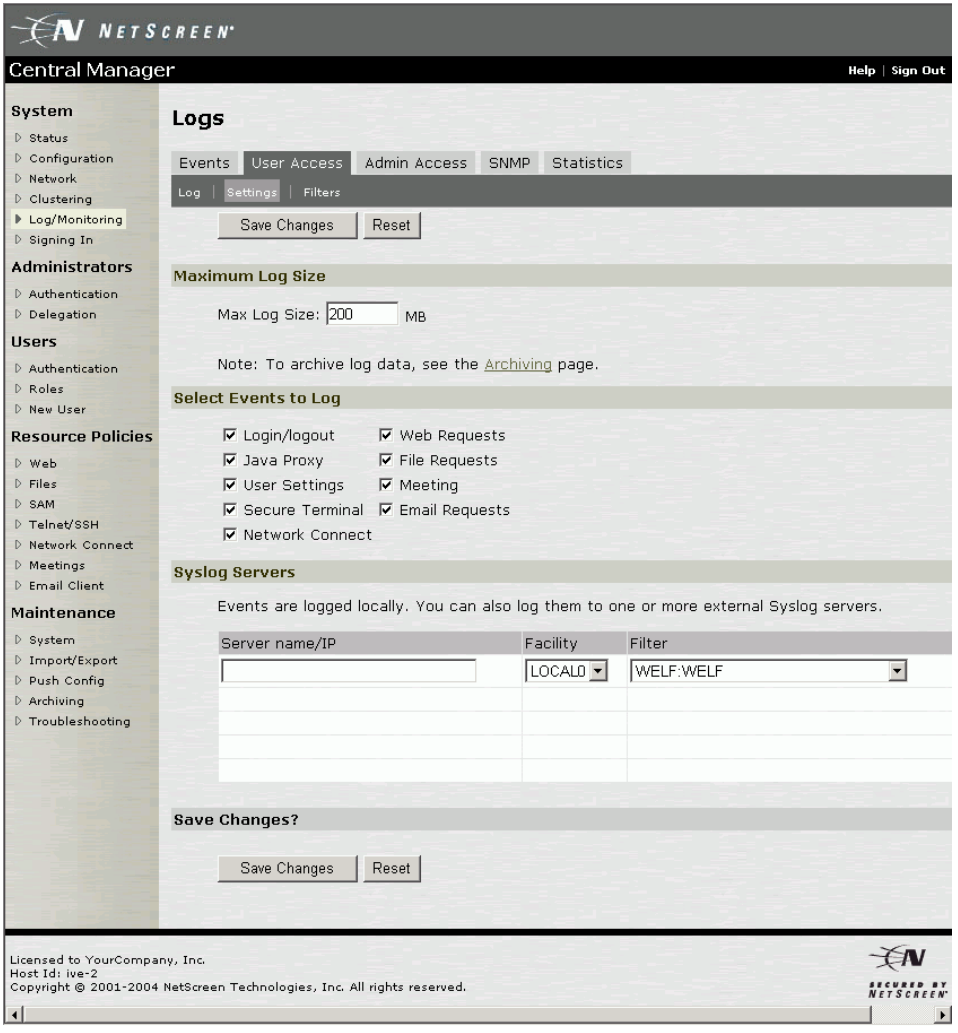


Abbildung 45: System > Log/Monitoring > User Access > Settings

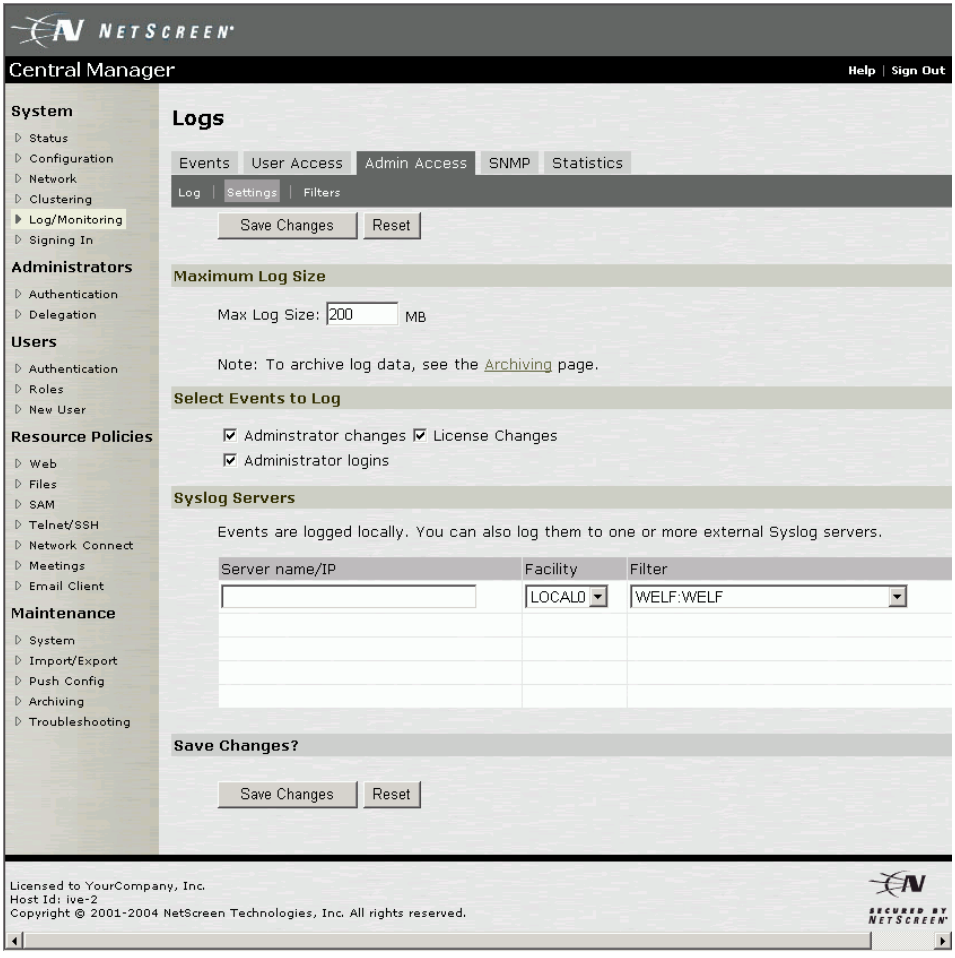


Abbildung 46: System > Log/Monitoring > Admin Access > Settings

Registerkarte „Filters“

☑ Erstellen von benutzerdefinierten Filtern und Formaten für Protokolldateien

Mithilfe der Optionen auf der Registerkarte **Filters** können Sie angeben, welche Daten in den Protokolldateien erfasst werden und welches Format verwendet wird. Diese Option ist nur mit dem Central Manager-Paket verfügbar.

1. Wählen Sie in der Webkonsole **System > Log/Monitoring** aus.
2. Klicken Sie auf die Registerkarte **Events**, **User Access** oder **Admin Access**, und wählen Sie dann **Filters** aus.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Um einen bestehenden Filter zu ändern, klicken Sie auf seinen Namen.
   - Um einen neuen Filter zu erstellen, klicken Sie auf **New Filter**.
4. Geben Sie eine Bezeichnung für den Filter ein.

   Wichtig: Wenn Sie ein Format auswählen und dann im Feld **Filter Name** eine neue Bezeichnung angeben, erstellt das IVE kein neues benutzerdefiniertes Filterformat, das auf dem bestehenden Format basiert. Stattdessen überschreibt es das bestehende Format mit den von Ihnen vorgenommenen Änderungen.

5. Klicken Sie auf **Make Default**, um den ausgewählten Filter als Standard-Protokolldateityp festzulegen. Sie können für die Ereignis-, Benutzerzugriffs- und Administratorzugriffsprotokolle jeweils unterschiedliche Standardfilter einstellen.
6. Anhand der Optionen im Abschnitt **Query** können Sie die Auswahl der Daten steuern, die das IVE ins Protokoll schreibt:
   1. Klicken Sie im Abschnitt **Start Date** auf **Earliest Date**, damit alle Protokolle ab dem ersten verfügbaren Datum geschrieben werden, das in der Protokolldatei gespeichert ist. Sie können auch manuell ein Startdatum eingeben.
   2. Klicken Sie im Abschnitt **End Date** auf **Latest Date**, damit alle Protokolle bis zum letzten verfügbaren Datum geschrieben werden, das in der Protokolldatei gespeichert ist. Sie können auch manuell ein Enddatum eingeben.
   3. Verwenden Sie die Sprache für benutzerdefinierte Ausdrücke des IVE im Abschnitt **Query**, um die Auswahl der Daten zu steuern, die das IVE ins Protokoll schreibt.

7. Sie können eine der Optionen aus dem Abschnitt **Export Format** verwenden, um das Datenformat im Protokoll zu steuern:
   - Wählen Sie die Option **Standard**, **WELF** oder **W3C** aus, um die Protokolleinträge mithilfe eines dieser standardisierten Formate zu formatieren. Weitere Informationen finden Sie unter „Benutzerdefinierte Filterung von Protokolldateien“ auf Seite 97.
   - Wählen Sie die Option **Custom** aus, und geben Sie das Format ein, das im Feld **Format** verwendet werden soll. Schließen Sie Variablen bei der Eingabe des Formats in Prozentzeichen ein (z. B. %user%). Alle anderen Zeichen im Feld werden als Literalzeichen behandelt.
8. Klicken Sie auf **Speichern**.

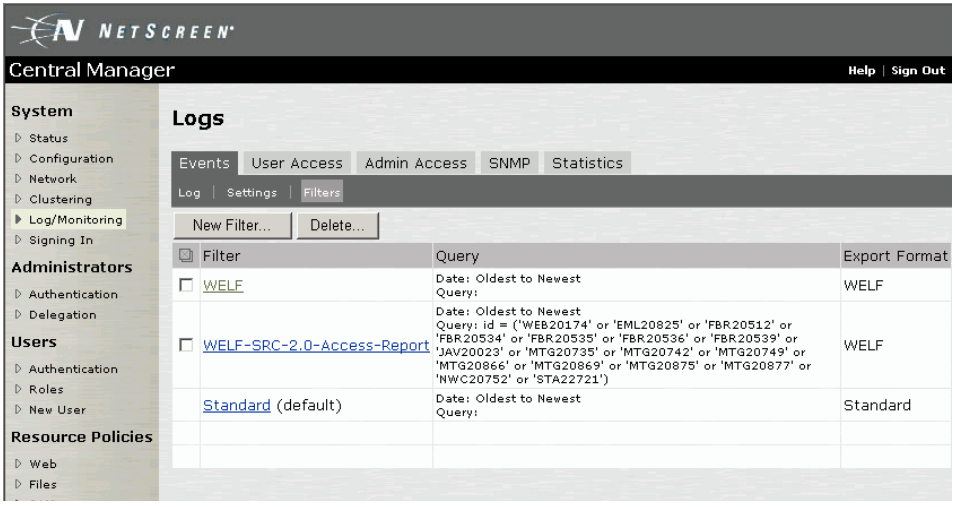


Abbildung 47: **System > Log/Monitoring > Events > Filters**

Registerkarte „SNMP“

☑ Überwachen des IVE als SNMP-Agent

Über diese Registerkarte können Sie ein Netzwerkverwaltungstool wie HP OpenView zum Überwachen des IVE als SNMP-Agent verwenden. Das IVE unterstützt SNMP (Simple Network Management Protocol), Version 2, implementiert eine private MIB (Management Information Base) und definiert eigene Traps. Um die Verarbeitung dieser Traps in der Netzwerkverwaltungsstation zu ermöglichen, müssen Sie die NetScreen-MIB-Datei herunterladen und die entsprechenden Angaben zum Empfangen der Traps machen.

Hinweis: Zum Überwachen wesentlicher IVE-Systemstatistiken, beispielsweise der CPU-Auslastung, laden Sie die UC-Davis-MIB-Datei in Ihre SNMP-Managementanwendung. Sie erhalten die MIB-Datei im Internet unter folgender Adresse: http://net-snmp.sourceforge.net/UCD-SNMP-MIB.txt.

So geben Sie SNMP-Einstellungen an:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > SNMP** aus.
2. Klicken Sie auf die Verknüpfung **NetScreenMIB file**, um auf die MIB-Datei zuzugreifen, und speichern Sie die Datei dann im Browser an einem Netzwerkspeicherort. (Eine Beschreibung der Get- und Trap-Objekte in der MIB-Datei finden Sie in den folgenden Tabellen.)
3. Geben Sie unter **Agent Properties** Informationen in die folgenden Felder ein, und klicken Sie anschließend auf **Save Changes**:
   - Geben Sie in die Felder **System Name**, **System Location** und **System Contact** Informationen ein, die den IVE-Agent beschreiben (optional).
   - Geben Sie im Feld **Community** eine Zeichenfolge ein (erforderlich).

     Hinweis: Zum Abfragen des IVEs muss Ihre Netzwerkverwaltungsstation diese Zeichenfolge an das IVE senden. Um den SNMP-Daemon zu beenden, löschen Sie die Angaben im Feld **Community**.
4. Legen Sie unter **Traps** die Server fest, an die das IVE Traps senden soll, die es bei Eingabe von Daten in die folgenden Felder generiert, und klicken Sie anschließend auf **Add**:
   - Der Hostname oder die IP-Adresse des Servers
   - Der Port, an dem der Server Daten abfragt (üblicherweise Port 162)
   - Die von der Netzwerkverwaltungsstation benötigte Community-Zeichenfolge (sofern vorhanden)
5. Klicken Sie auf **Save Changes**.
6. Gehen Sie in der Netzwerkverwaltungsstation folgendermaßen vor:
   1. Laden Sie die NetScreen-MIB-Datei herunter.
   2. Geben Sie die Community-Zeichenfolge an, die beim Abfragen des IVE benötigt wird (siehe Schritt 3).
   3. Konfigurieren Sie die Netzwerkverwaltungssoftware für den Empfang von IVE-Traps.

Tabelle 2: NetScreen-MIB-Objekte: Gets

Objekt	Beschreibung
logFullPercent	Gibt den Prozentsatz der verfügbaren Dateigröße zurück, der durch das aktuelle Protokoll belegt wird.
signedInWebUsers	Gibt die Anzahl der über einen Webbrowser beim IVE angemeldeten Benutzer zurück.
signedInMailUsers	Gibt die Anzahl der am E-Mail-Client angemeldeten Benutzer zurück.
productName	Gibt den Produktnamen des lizenzierten IVE zurück.
productVersion	Gibt die Softwareversion des IVE-Systems zurück.

Tabelle 3: NetScreen-MIB-Objekte: Traps

Objekt	Beschreibung
iveLogNearlyFull	Eines der Protokolle (System, Benutzerzugriff oder Administratorenzugriff) ist zu 90% voll. Wenn dieses Trap gesendet wird, wird auch der Parameter `logFullPercent` (Protokolldatei ist zu % voll) gesendet.
iveLogFull	Eines der Protokolle (System, Benutzerzugriff oder Administratorenzugriff) ist restlos voll.
iveMaxConcurrentUsersSignedIn	Höchstanzahl oder zulässige Anzahl gleichzeitig angemeldeter Benutzer ist angemeldet, plus 10 %.

Tabelle 3: NetScreen-MIB-Objekte: Traps (Fortsetzung)

Objekt	Beschreibung
iveTooManyFailedLoginAttempts	Für die angegebene IP-Adresse sind zu viele fehlgeschlagene Anmeldeversuche ausgeführt worden. Wird ausgelöst, wenn die Authentifizierung eines Benutzers im Verlauf einer Stunde 180-mal fehlschlägt. Nach dem Empfang dieser Meldung wird die IP-Adresse des Benutzers für 2 Minuten gesperrt, bevor seine Anmeldung wieder zulässig ist. Wenn dann der Anmeldevorgang des Benutzers innerhalb von 30 Minuten 90-mal fehlschlägt, wird seine IP-Adresse erneut gesperrt. Dieser Zyklus wird fortgesetzt, wobei der Zeitraum und die Anzahl fehlgeschlagener Anmeldeversuche jeweils halbiert wird. Im dritten Zyklus wird der Benutzer nach 45 fehlgeschlagenen Anmeldeversuchen innerhalb von 15 Minuten gesperrt, im vierten Zyklus nach 23 fehlgeschlagenen Anmeldeversuchen innerhalb von 8 Minuten usw. Wenn dieses Trap gesendet wird, wird auch der Parameter `blockedIP` (Quell-IP der Anmeldeversuche) gesendet.
externalAuthServerUnreachable	Ein externer Authentifizierungsserver beantwortet keine Authentifizierungsanforderungen. Wenn dieses Trap gesendet wird, wird auch der Parameter `authServerName` (Name des nicht erreichbaren Servers) gesendet.
iveStart	IVE wurde soeben eingeschaltet.
iveShutdown	IVE wurde soeben heruntergefahren.
iveReboot	IVE wurde soeben neu gestartet.
archiveServerUnreachable	IVE kann den konfigurierten FTP-Archivierungsserver nicht erreichen.
archiveServerLoginFailed	IVE kann sich nicht beim konfigurierten FTP-Archivierungsserver anmelden.
archiveFileTransferFailed	IVE kann keine erfolgreiche Übertragung des Archivs auf den konfigurierten FTP-Archivierungsserver ausführen.

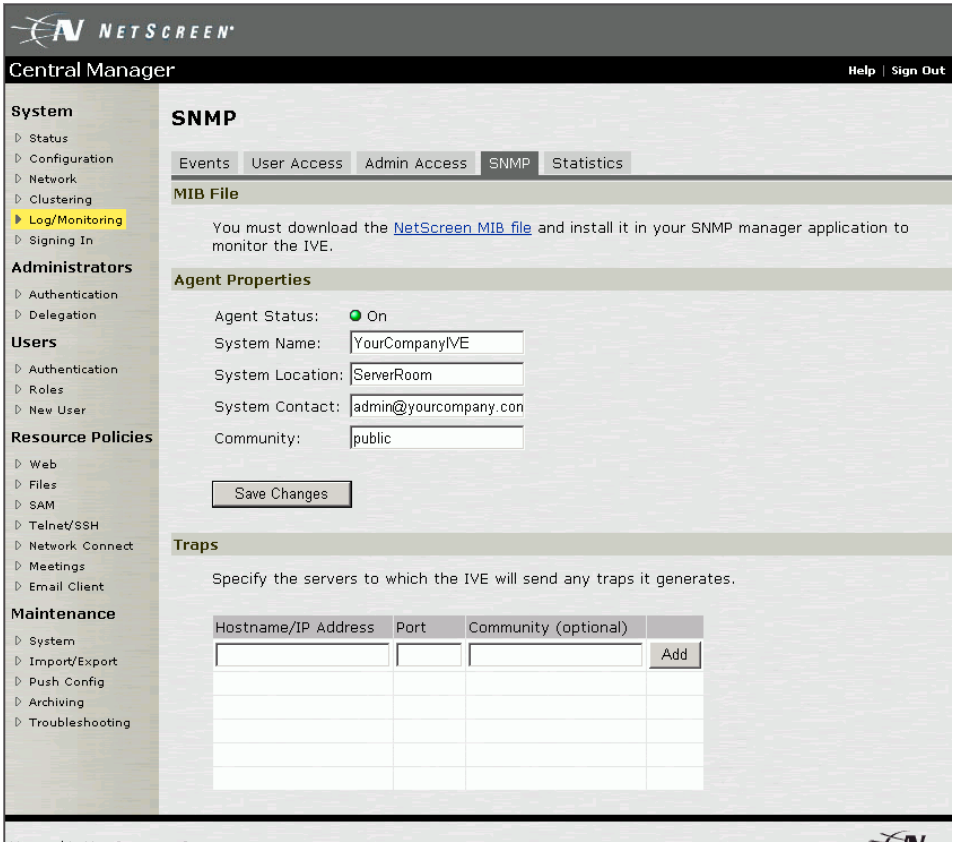


Abbildung 48: System > Log/Monitoring > SNMP

Registerkarte „Statistics“

☑ Anzeigen der Systemstatistik

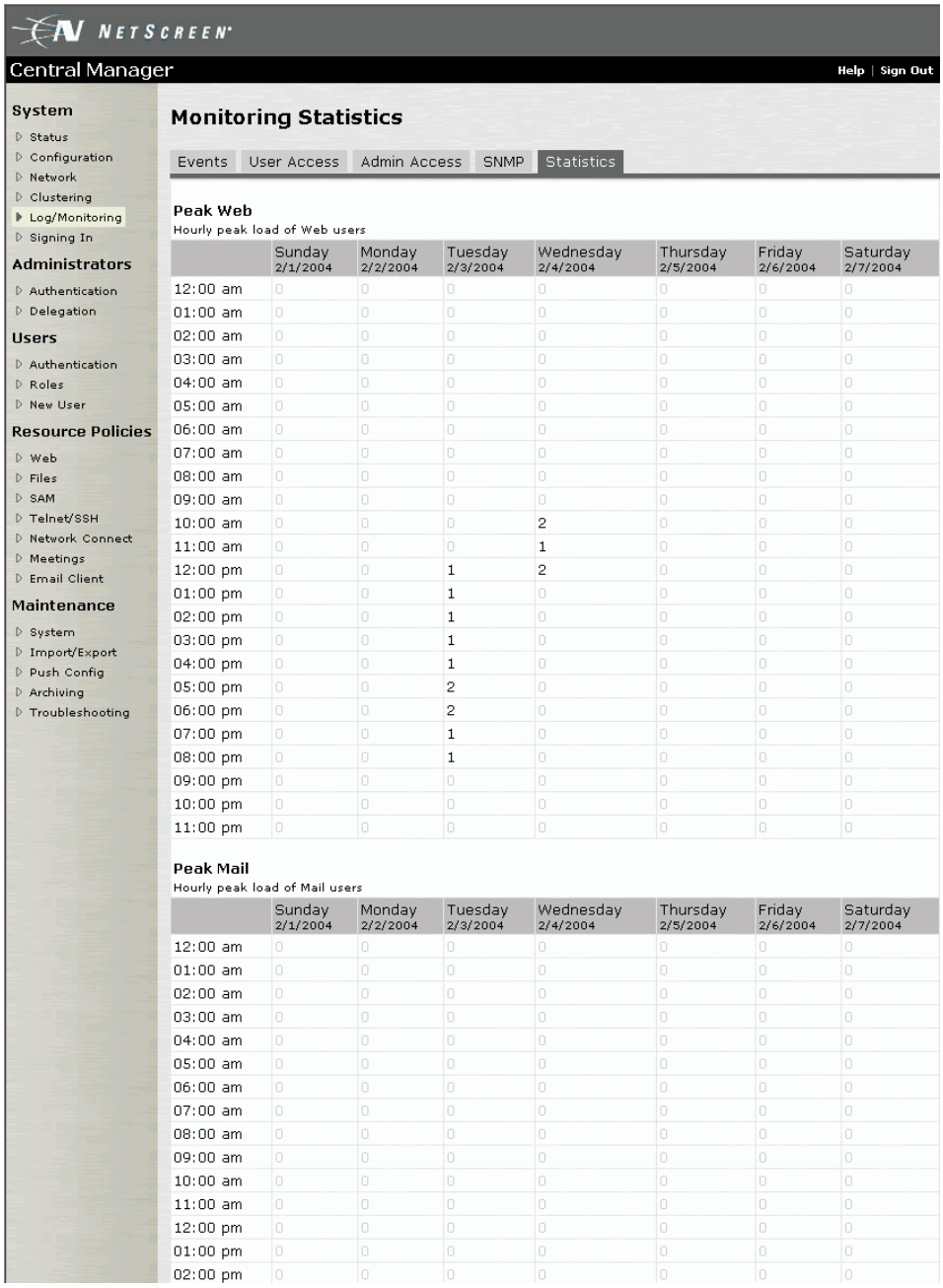
Das IVE protokolliert stündlich die folgenden Daten:

- Spitzenbelastung durch Webbenutzer
- Spitzenbelastung durch E-Mail-Benutzer
- Anzahl der URLs, auf die zugegriffen wird
- Anzahl der Dateien, auf die zugegriffen wird

Auf der Seite **Statistics** werden die Informationen für die letzten sieben Tage angezeigt. Diese Informationen werden einmal wöchentlich in das Systemprotokoll geschrieben. Beim Aktualisieren des IVE werden alle Statistiken gelöscht. Wenn Sie das System so konfigurieren, dass es stündlich die Statistik protokolliert, sind die alten Statistiken nach einer Aktualisierung immer noch in der Protokolldatei verfügbar.

So zeigen Sie die Systemstatistik an:

1. Wählen Sie in der Webkonsole **System > Log/Monitoring > Statistics** aus.
2. Führen Sie auf der Seite einen Bildlauf durch, um alle vier Datenkategorien anzuzeigen.



	Sunday 2/1/2004	Monday 2/2/2004	Tuesday 2/3/2004	Wednesday 2/4/2004	Thursday 2/5/2004	Friday 2/6/2004	Saturday 2/7/2004
12:00 am	0	0	0	0	0	0	0
01:00 am	0	0	0	0	0	0	0
02:00 am	0	0	0	0	0	0	0
03:00 am	0	0	0	0	0	0	0
04:00 am	0	0	0	0	0	0	0
05:00 am	0	0	0	0	0	0	0
06:00 am	0	0	0	0	0	0	0
07:00 am	0	0	0	0	0	0	0
08:00 am	0	0	0	0	0	0	0
09:00 am	0	0	0	0	0	0	0
10:00 am	0	0	0	2	0	0	0
11:00 am	0	0	0	1	0	0	0
12:00 pm	0	0	1	2	0	0	0
01:00 pm	0	0	1	0	0	0	0
02:00 pm	0	0	1	0	0	0	0
03:00 pm	0	0	1	0	0	0	0
04:00 pm	0	0	1	0	0	0	0
05:00 pm	0	0	2	0	0	0	0
06:00 pm	0	0	2	0	0	0	0
07:00 pm	0	0	1	0	0	0	0
08:00 pm	0	0	1	0	0	0	0
09:00 pm	0	0	0	0	0	0	0
10:00 pm	0	0	0	0	0	0	0
11:00 pm	0	0	0	0	0	0	0

	Sunday 2/1/2004	Monday 2/2/2004	Tuesday 2/3/2004	Wednesday 2/4/2004	Thursday 2/5/2004	Friday 2/6/2004	Saturday 2/7/2004
12:00 am	0	0	0	0	0	0	0
01:00 am	0	0	0	0	0	0	0
02:00 am	0	0	0	0	0	0	0
03:00 am	0	0	0	0	0	0	0
04:00 am	0	0	0	0	0	0	0
05:00 am	0	0	0	0	0	0	0
06:00 am	0	0	0	0	0	0	0
07:00 am	0	0	0	0	0	0	0
08:00 am	0	0	0	0	0	0	0
09:00 am	0	0	0	0	0	0	0
10:00 am	0	0	0	0	0	0	0
11:00 am	0	0	0	0	0	0	0
12:00 pm	0	0	0	0	0	0	0
01:00 pm	0	0	0	0	0	0	0
02:00 pm	0	0	0	0	0	0	0

Abbildung 49: System > Log/Monitoring > Statistics

Konfigurieren der Seite „Signing-in“

Die Seite **System > Signing-in** enthält die folgenden Registerkarten:

Registerkarte „Sign-in Policies“ 203
Registerkarte „Sign-in Page“ 209
Registrierkarte „Server“ 212

Auf der Seite **System > Signing-in** können Sie Folgendes durchführen:

Erstellen und Konfigurieren von Anmelderichtlinien 204
Legen Sie die Reihenfolge fest, in der die Anmelderichtlinien ausgewertet werden. 206
Aktivieren und Deaktivieren von Anmelderichtlinien 208
Ändern der Standardanmeldeseite 209
Hochladen einer benutzerdefinierten Anmeldeseite 212
Definieren einer Authentifizierungsserverinstanz 213

Registerkarte „Sign-in Policies“

Anmelderichtlinien legen die URLs fest, die Benutzer und Administratoren für den Zugriff auf das IVE verwenden können. Bei der Konfiguration einer Anmelderichtlinie müssen Sie diese mindestens einem Bereich zuordnen. Es können sich dann nur Mitglieder des/der angegebenen Authentifizierungsbereiche(s) über den URL anmelden, der in der Richtlinie festgelegt ist. Sie können in der Anmelderichtlinie auch unterschiedliche Anmeldeseiten festlegen und sie unterschiedlichen URLs zuordnen.

So können Sie z. B Anmelderichtlinien erstellen, die Folgendes angeben:

- Mitglieder des Bereichs „Partner“ können sich über folgende URLs beim IVE anmelden: `partner1.eigenefirma.com` und `partner2.eigenefirma.com`. Für Benutzer, die sich über den ersten URL anmelden, öffnet sich die Anmeldeseite „partner1“; für Benutzer, die sich über den zweiten URL anmelden, öffnet sich die Anmeldeseite „partner2“.
- Mitglieder der Bereiche „Lokal" und „Remote“ können sich über den folgenden URL beim IVE anmelden: `mitarbeiter.eigenefirma.com`. Bei der Anmeldung wird die Anmeldeseite „Mitarbeiter“ geöffnet.
- Mitglieder des Bereichs „Admin Users“ können sich über den folgenden URL beim IVE anmelden: `zugriff.eigenefirma.com/super`. Bei der Anmeldung wird die Anmeldeseite „Administratoren“ geöffnet.

Beim Festlegen von Anmelderichtlinien können Sie verschiedene Hostnamen verwenden (z.B. `partner.eigenefirma.com` und `mitarbeiter.eigenefirma.com`) oder verschiedene Pfade (z.B. `eigenefirma.com/partner` und `eigenefirma.com/mitarbeiter`), um zwischen den URLs zu unterscheiden.

Wichtig: Wenn Sie die URLs anhand von Hostnamen unterscheiden, müssen Sie über die Seite **System > Configuration > Certificates > Server Certificates** ein Platzhalterzertifikat auf das IVE hochladen.

☑ Erstellen und Konfigurieren von Anmelderichtlinien

1. Wählen Sie in der Webkonsole **System > Signing In > Sign-in Policies** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **New**, um eine neue Richtlinie zu erstellen.
   - Klicken Sie auf einen URL in der Spalte **Administrator URLs** oder **User URLs**, um eine vorhandene Richtlinie zu bearbeiten.
3. Wählen Sie **Users** oder **Administrators** aus, um anzugeben, welcher Typ von Benutzer sich mithilfe dieser Richtlinie beim IVE anmelden kann.
4. Geben Sie im Feld **Sign-in URL** den URL ein, die Sie der Richtlinie zuordnen möchten.
   - Um anzugeben, dass alle Administrator-URLs innerhalb des festgelegten Bereichs bzw. der festgelegten Bereiche die Anmeldeseite verwenden müssen, geben Sie ***/admin** ein.
   - Um anzugeben, dass alle Endbenutzer-URLs innerhalb des festgelegten Bereichs bzw. der festgelegten Bereiche die Anmeldeseite verwenden müssen, geben Sie ***/** ein.

   Hinweis: Im Hostnamenabschnitt des URL können Sie nur Platzhalterzeichen (*) verwenden. Das IVE erkennt keine Platzhalter im URL-Pfad.

   ---
5. Geben Sie unter **Description** eine Beschreibung für die Richtlinie ein (optional).
6. Wählen Sie unter **Sign-in page** eine Anmeldeseite aus. Sie können die Standardseite für das IVE auswählen, eine Variation der Standardanmeldeseite oder eine benutzerdefinierte Seite, die Sie mithilfe der Funktion „Customizable UI" erstellen. Weitere Informationen finden Sie unter „Registerkarte „Sign-in Page"" auf Seite 209.
7. Legen Sie unter **Authentication realm** fest, welche Bereiche der Richtlinie zugeordnet sein sollen und wie Benutzer und Administratoren unter den Bereichen auswählen sollen. Wenn Sie Folgendes auswählen:

- **User types the realm name**

  Die Anmelderichtlinie wird allen Authentifizierungsbereichen zugeordnet, das IVE stellt jedoch keine Bereichsliste bereit, aus der ein Benutzer oder Administrator auswählen kann. Stattdessen muss der Benutzer oder Administrator seinen Bereichsnamen manuell auf der Anmeldeseite eingeben.

- **User picks from a list of authentication realms**

  Die Anmelderichtlinie ist nur dem von Ihnen gewählten Authentifizierungsbereich zugeordnet. Das IVE zeigt dem Benutzer oder Administrator diese Bereichsliste bei der Anmeldung am IVE an und ermöglicht die Auswahl eines in der Liste aufgeführten Bereichs. (Wenn dem URL nur ein einziger Bereich zugeordnet ist, zeigt das IVE keine Dropdownliste von Bereichen an. Stattdessen verwendet es automatisch den von Ihnen festgelegten Bereich.)

8. Klicken Sie auf **Save Changes**.

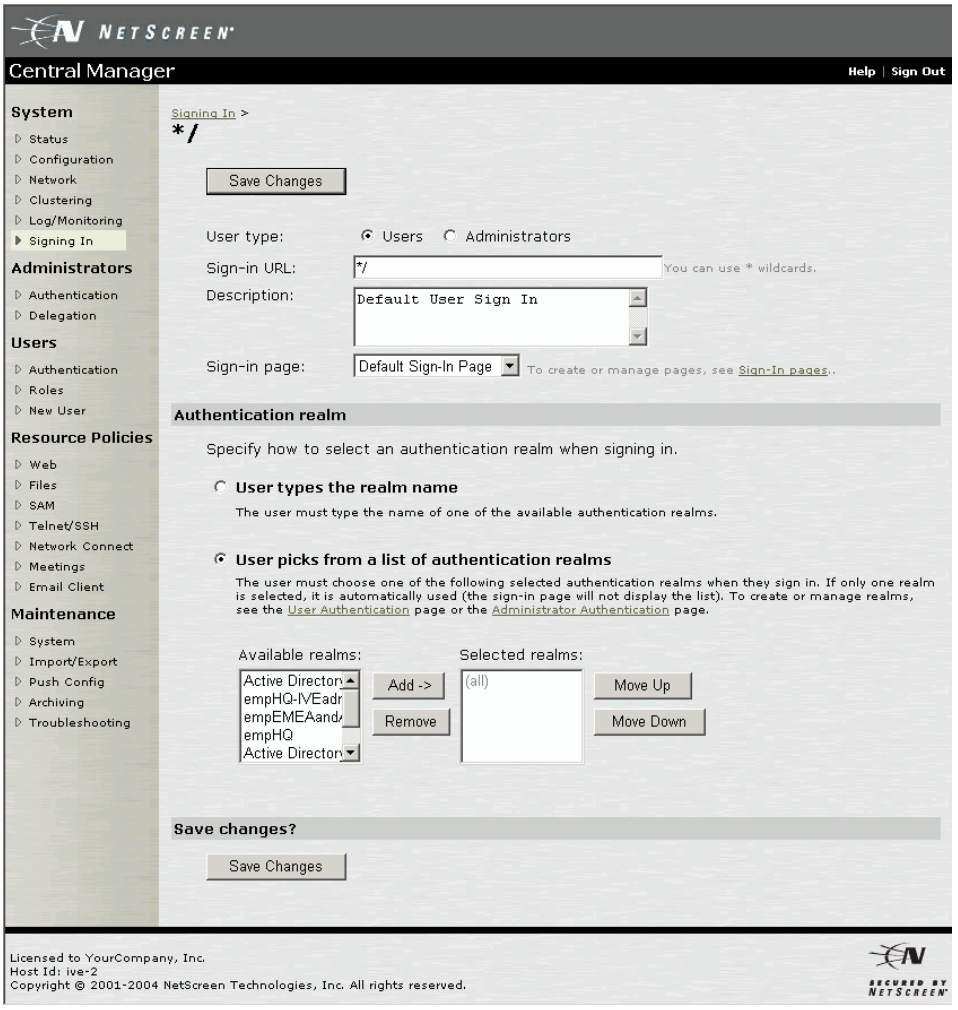


Abbildung 50: System > Signing In > Sign-in Policies > [Ausgewählte Richtlinie]

☑ Legen Sie die Reihenfolge fest, in der die Anmelderichtlinien ausgewertet werden

Das IVE wertet die Anmelderichtlinien für Administratoren in der gleichen Reihenfolge aus, in der sie auf der Seite **Sign-in Policies** aufgeführt sind, und wertet dann die Anmelderichtlinien für Benutzer aus. Wenn es einen exakt übereinstimmenden URL findet, bricht es die Auswertung ab und öffnet die entsprechende Anmeldeseite für den Administrator bzw.

Benutzer. Sie können z.B. zwei Administrator-Anmelderichtlinien mit zwei verschiedenen URLs festlegen:

- Die erste Richtlinie verwendet den URL `*/admin` und ordnet die Standardanmeldeseite für Administratoren zu.
- Die zweite Richtlinie verwendet den URL `eigenefirma.com/admin` und ordnet eine benutzerdefinierte Anmeldeseite für Administratoren zu.

Wenn Sie die Richtlinien auf der Seite **Sign-in Policies** in dieser Reihenfolge aufführen, wertet das IVE die zweite Richtlinie niemals aus bzw. verwendet sie nie, da der erste URL den zweiten einschließt. Selbst bei der Anmeldung eines Administrators über den URL `eigenefirma.com/admin` zeigt das IVE die Standardanmeldeseite für Administratoren an. Wenn Sie die Richtlinien hingegen in umgekehrter Reihenfolge aufführen, zeigt das IVE die benutzerdefinierte Anmeldeseite allen Administratoren an, die über den URL `eigenefirma.com/admin` auf das IVE zugreifen.

Das IVE akzeptiert nur Platzhalterzeichen im Hostnamenabschnitt des URL und ordnet den URL anhand des exakten Pfades zu. Sie können z.B. zwei Administrator-Anmelderichtlinien mit zwei verschiedenen URL-Pfaden festlegen:

- Die erste Richtlinie verwendet den URL `*/marketing` und ordnet eine benutzerdefinierte Anmeldeseite für die gesamte Marketingabteilung zu.
- Die zweite Richtlinie verwendet den URL `*/marketing/joe` und ordnet eine benutzerdefinierte Anmeldeseite zu, die ausschließlich für den Mitarbeiter „Joe" der Marketingabteilung vorgesehen ist.

Wenn Sie die Richtlinien auf der Seite **Sign-in Policies** in dieser Reihenfolge aufführen, zeigt das IVE die benutzerdefinierte Anmeldeseite für Joe immer dann an, wenn Joe über den URL `eigenefirma.com/marketing/joe` auf das IVE zugreift. Joe wird die Marketinganmeldeseite nicht angezeigt, obwohl sie als erste aufgeführt und ausgewertet wird, da der Pfadabschnitt seines URL nicht genau mit dem URL übereinstimmt, der in der ersten Richtlinie definiert ist.

So ändern Sie die Reihenfolge, in der die Anmelderichtlinien für Administratoren ausgewertet werden:

1. Wählen Sie in der Webkonsole **System > Signing In > Sign-in Policies** aus.
2. Wählen Sie eine Anmelderichtlinie aus der Liste **Administrator URL** aus.
3. Ändern Sie die Position der Richtlinie in der Liste mithilfe der Pfeile nach oben oder nach unten.
4. Klicken Sie auf **Save Changes**.

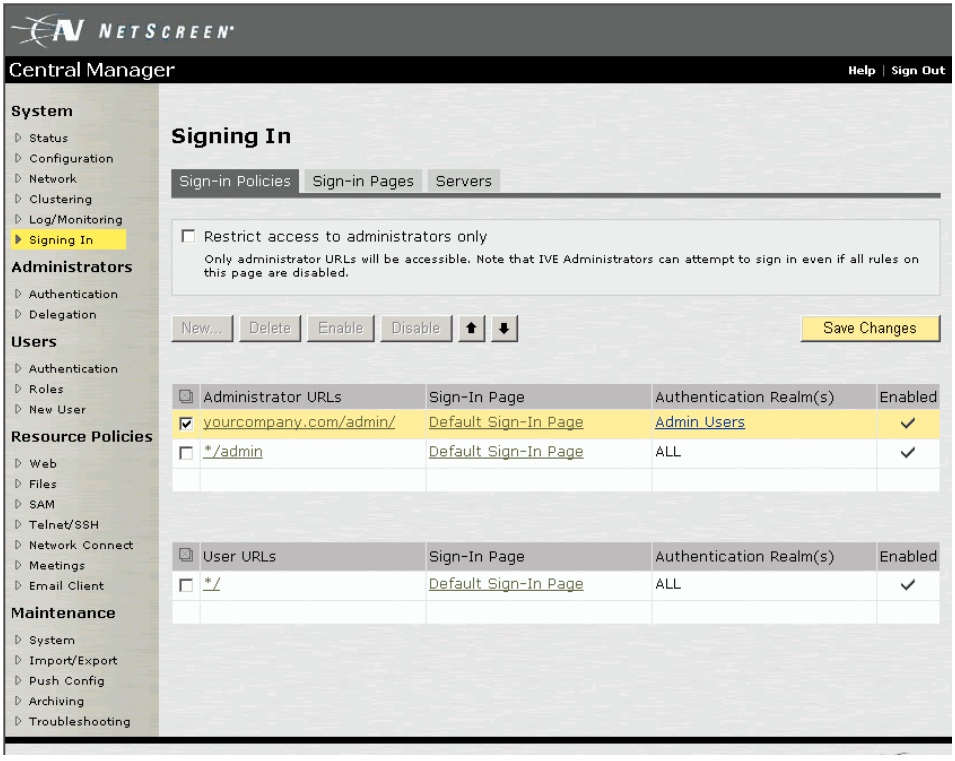


Abbildung 51: System > Signing In > Sign-in Policies (Änderung der Reihenfolge)

☑ Aktivieren und Deaktivieren von Anmelderichtlinien

So aktivieren und deaktivieren Sie Anmelderichtlinien:

1. Wählen Sie in der Webkonsole **System > Signing In > Sign-in Policies** aus.
2. So gehen Sie für die Aktivierung oder Deaktivierung vor:
   - **Einzelne Richtlinie** – Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie ändern möchten, und klicken Sie dann auf **Enable** oder **Disable**.
   - **Alle Benutzerrichtlinien** – Aktivieren oder deaktivieren Sie das Kontrollkästchen **Restrict access to administrators only**.

Registerkarte „Sign-in Page“

Eine Anmeldeseite legt die benutzerdefinierten Eigenschaften der Willkommensseite des Benutzers fest, wie etwa Begrüßungstext, Hilfetext, Logo, Kopf- und Fußbereich. Das IVE ermöglicht es Ihnen, Benutzern und Administratoren zwei Arten von Anmeldeseiten anzuzeigen.

- **Standardanmeldeseiten**

  Die Standardanmeldeseiten sind NetScreen vorgegeben und sind in allen Versionen des IVE enthalten. Beachten Sie, dass auch die Seiten, die über die Registerkarte **System > Signing In > Sign-in Page** geändert werden, als Standardanmeldeseiten zählen.

- **Benutzerdefinierte Anmeldeseiten**

  Benutzerdefinierte Anmeldeseiten sind THTML-Seiten, die Sie mithilfe des Template Toolkit erstellen und in Form einer archivierten ZIP-Datei in das IVE hochladen. Die Erstellung von benutzerdefinierten Anmeldeseiten ist eine lizenzierte Funktion, die es Ihnen ermöglicht, anstelle der geänderten IVE-Anmeldeseite eigene Seiten zu verwenden. Für die Erstellung benutzerdefinierter Anmeldeseiten stehen Ihnen unter `www.support.netscreen.com` Vorlagen und Dokumentation zur Verfügung.

☑ Ändern der Standardanmeldeseite

So ändern Sie die IVE-Standardanmeldeseite:

1. Wählen Sie in der Webkonsole **System > Signing In > Sign-in Pages** aus.
2. Klicken Sie auf **New**.
3. Geben Sie einen Namen ein, um die Seite zu bezeichnen.
4. Ändern Sie in den Abschnitten **Custom Text** und **Custom Error Messages** den für die verschiedenen Fensterbeschriftungen verwendeten Standardtext nach Bedarf.
5. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
6. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Show Help Button** aus, geben Sie eine Beschriftung für die Schaltfläche ein, und geben Sie eine HTML-Datei an, die in das IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die in dieser HTML-Seite verwiesen wird.

7. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.

Hinweis: Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Benutzer und der Webkonsole zurückzusetzen.

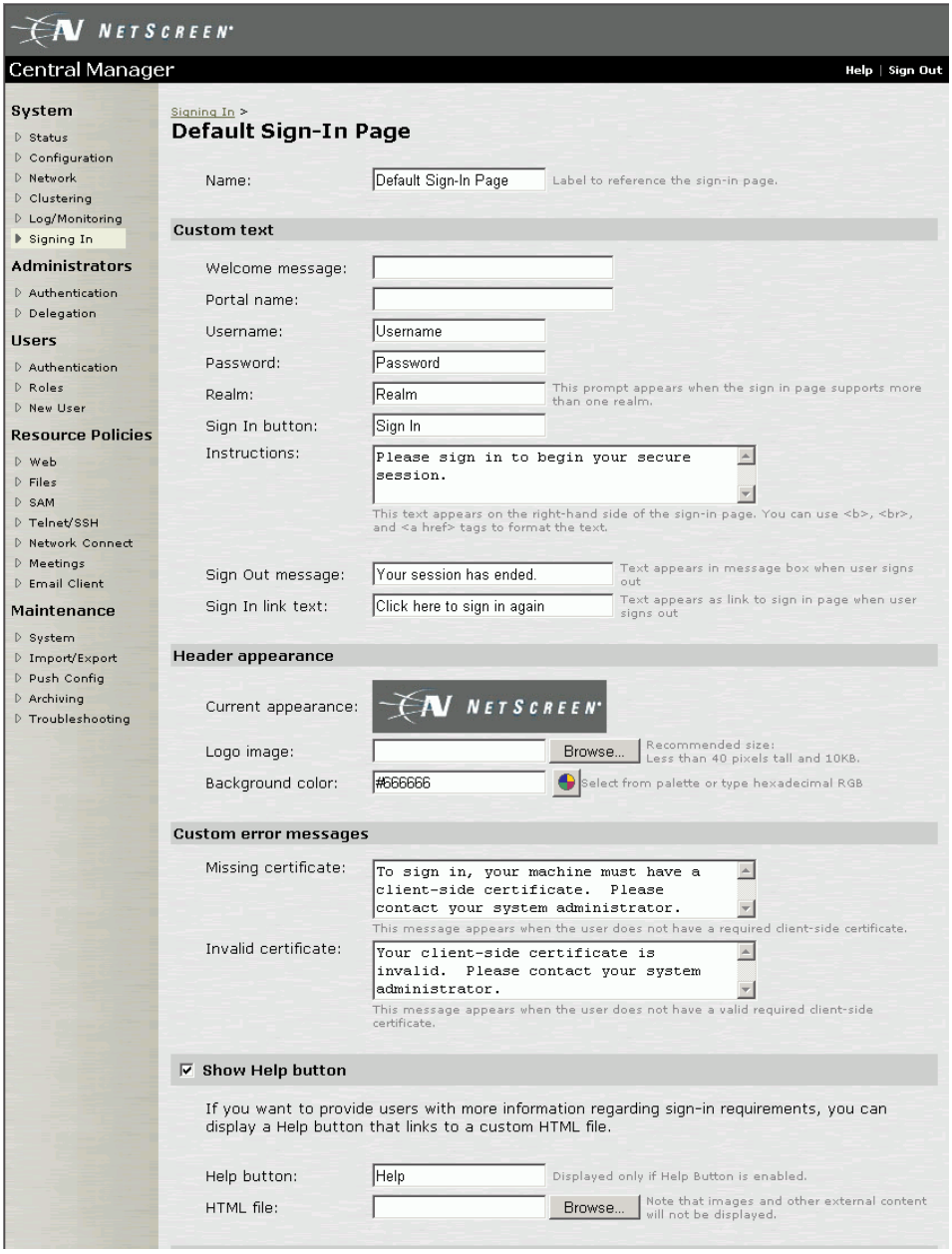


Abbildung 52: System > Signing In > Sign-in Policies > [Ausgewählte Seite]

☑ Hochladen einer benutzerdefinierten Anmeldeseite

So laden Sie benutzerdefinierte Seiten in das IVE hoch:

1. Wählen Sie in der Webkonsole **System > Signing In > Sign-in Pages** aus.
2. Klicken Sie auf **Upload Custom Pages**.
3. Geben Sie einen Namen ein, um die Seite zu bezeichnen.
4. Navigieren Sie im Browser zu der ZIP-Datei, die Ihre benutzerdefinierte(n) Seite(n) enthält.

   Hinweis: Für die Erstellung benutzerdefinierter Anmeldeseiten stehen Ihnen unter „www.support.netscreen.com“ Vorlagen und Dokumentation zur Verfügung.

5. Klicken Sie auf **Save Changes**.

Registrierkarte „Server“

Authentifizierungsserver authentifizieren Anmeldeinformationen der Benutzer, während Autorisierungsserver Benutzerinformationen bereitstellen, die das IVE zur Ermittlung von Benutzerberechtigungen im System verwendet. Sie können z. B. eine Zertifikatserverinstanz angeben, die Benutzer anhand ihrer clientseitigen Zertifikatsattribute authentifiziert, und dann eine LDAP-Serverinstanz erstellen, die Benutzer anhand der Werte autorisiert, die in einer Zertifikatsperrliste (Certificate Revocation List, CRL) aufgeführt sind. Weitere Informationen zu Authentifizierungsservern finden Sie unter „Authentifizierungsserver“ auf Seite 35.

☑ Definieren einer Authentifizierungsserverinstanz

So definieren Sie eine Serverinstanz:

1. Geben Sie Einstellungen für die individuelle Serverinstanz an. Anweisungen hierfür finden Sie unter:
   - Konfigurieren einer ACE/Serverinstanz (215)
   - Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz (221)
   - Konfigurieren einer Instanz eines anonymen Servers (223)
   - Konfigurieren einer Zertifikatserverinstanz (225)
   - Konfigurieren einer LDAP-Serverinstanz (229)
   - Konfigurieren einer lokalen IVE-Server-Instanz (235)
   - Konfigurieren einer Netegrity SiteMinder-Instanz (247)
   - Konfigurieren einer NIS-Serverinstanz (241)
   - Konfigurieren einer RADIUS-Serverinstanz (243)

   Hinweis: Beachten Sie bei der Auswahl des Servertyps Folgendes:
   - Sie können nur eine ACE- und eine RADIUS-Serverinstanz pro IVE erstellen.
   - Sie können den Active Directory-Server mit folgenden Protokollen authentifizieren:
     - **NTLM-Protokoll** – Wählen Sie **Active Directory/Windows NT Domain**(Seite 221) aus.
     - **LDAP-Protokoll** – Wählen Sie **LDAP Server** (Seite 229) aus.
   - Wenn Sie eine Serverinstanz zum Authentifizieren von Benutzeradministratoren erstellen (Seite 238), müssen Sie **IVE Authentication** auswählen.
2. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).
3. Wenn Sie den lokalen IVE-Authentifizierungsserver konfigurieren, müssen Sie lokale Benutzerkonten festlegen. Anweisungen hierfür finden Sie unter „Erstellen lokaler Benutzer“ auf Seite 236.

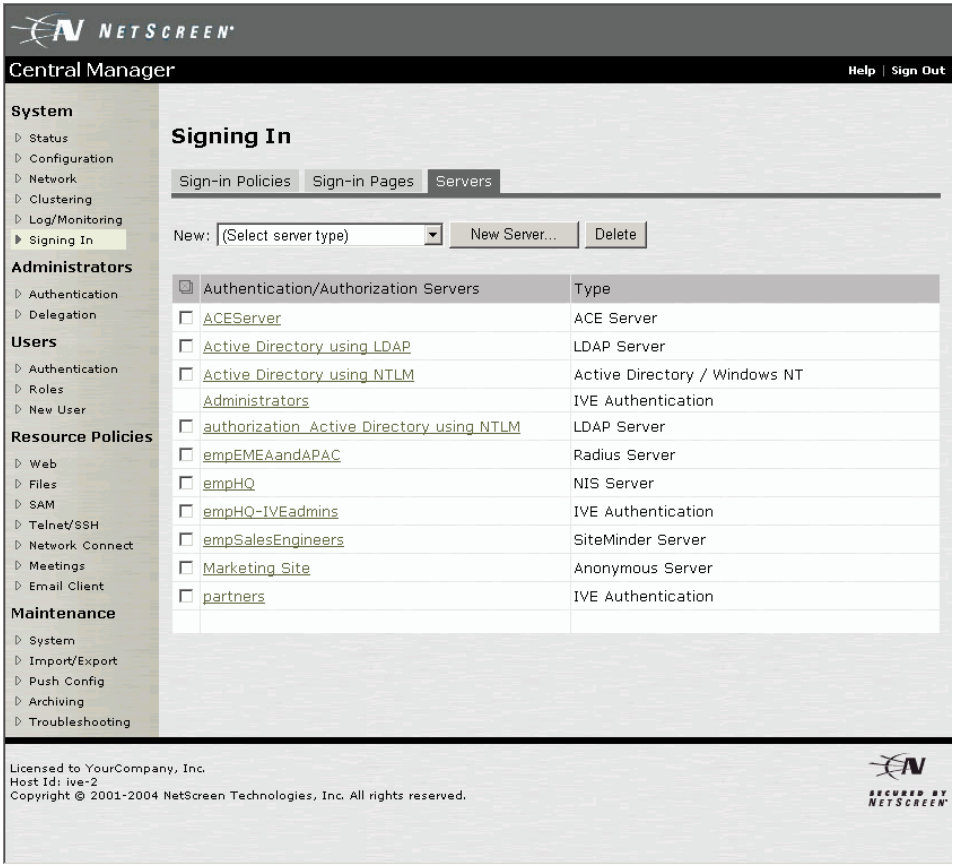


Abbildung 53: System > Signing In > Servers

Konfigurieren einer ACE/Serverinstanz

Die folgenden Themen werden behandelt:

ACE/Server – Übersicht 215
Definieren einer ACE/Serverinstanz 216
Generieren einer ACE/Agent-Konfigurationsdatei 219

ACE/Server – Übersicht

Wenn die Benutzerauthentifizierung über einen RSA ACE/Server erfolgt, können sich Benutzer mit zwei Methoden anmelden:

- **Unter Verwendung der IVE-Standardanmeldeseite:**
  Der Benutzer wechselt zur Standardanmeldeseite für das IVE, und gibt dann den Benutzernamen und das Kennwort ein (bestehend aus der Kombination von PIN und dem aktuellen Wert des RSA SecurID-Hardware- oder Softwaretokens). Das IVE leitet diese Anmeldeinformationen des Benutzers dann an ACE/Server weiter.
- **Unter Verwendung der RSA SecurID-Authentifizierungsseite:**
  Wenn der Benutzer RSA SecurID-Software im System installiert hat, kann er unter Verwendung des folgenden URL-Formats auf die Seite **RSA SecurID Authentication** wechseln: `https://IVE/login/ServerInstanz` und Eingabe der PIN. (In Abhängigkeit von der RSA-Konfiguration muss der Benutzer möglicherweise auch den Benutzernamen eingeben.) Wenn die IVE-Appliance die Gültigkeit der Anmeldeanforderung bestätigt hat, kann die RSA SecurID-Software einen Tokenwert transparent über die IVE-Appliance an ACE/Server weitergeben.

Wenn ACE/Server den Benutzer authentifiziert hat, wird der Zugriff auf die IVE-Appliance gewährt. Andernfalls führt ACE/Server folgende Aktionen aus:

- **Verweigern des Benutzerzugriffs auf das System**
  wenn die Anmeldeinformationen des Benutzers nicht erkannt wurden.
- **Weiterleiten des Benutzers an die IVE-Standardanmeldeseite**
  wenn der Benutzer versucht, sich auf der Seite **RSA SecurID Authentication** auf einem Computer anzumelden, auf dem die SecurID-Software nicht installiert ist.
- **Auffordern des Benutzers, eine neue PIN zu erstellen (New PIN-Modus)**
  wenn der Benutzer sich erstmals bei NetScreen Instant Virtual Extranet anmeldet. (Dem Benutzer werden je nach verwendetem Anmeldeverfahren unterschiedliche Aufforderungen angezeigt. Bei Anmeldung über die

Seite **RSA SecurID Authentication** werden die RSA-Aufforderungen zum Erstellen einer neuen PIN angezeigt. Andernfalls werden die IVE-Aufforderungen angezeigt.) Beachten Sie, dass der Benutzer für die erstmalige Anmeldung eine temporäre PIN benötigt.

- **Auffordern des Benutzers zur Eingabe des nächsten Tokens (Next Token-Modus)**
  wenn das vom Benutzer eingegebene Token nicht mit dem von ACE/Server erwarteten Token übereinstimmt. (Der Next Token-Modus ist für Benutzer transparent, die sich über die Seite **RSA SecurID Authentication** anmelden. Die RSA SecurID-Software übergibt das Token über die IVE-Appliance und ohne Benutzerinteraktion an ACE/Server.)

Wenn der Benutzer die neue PIN oder das nächste Token eingibt (je nach Modus), bleiben drei Minuten für die Eingabe der erforderlichen Informationen. Danach bricht das IVE die Transaktion ab und fordert den Benutzer zur erneuten Eingabe der Anmeldeinformationen auf.

Das IVE kann bis zu 200 ACE/Server-Transaktionen gleichzeitig verarbeiten. Eine Transaktion dauert nur so lange wie die Authentifizierung bei ACE/Server. Wenn sich ein Benutzer z.B. am IVE anmeldet, wird die ACE/Server-Transaktion beim Senden der Anforderung durch den Benutzer initiiert. Die Transaktion wird beendet, sobald ACE/Server die Verarbeitung der Anforderung beendet hat. Der Benutzer kann mit der IVE-Sitzung fortfahren, obwohl die ACE/Server-Transaktion beendet wurde.

Das IVE unterstützt die folgenden ACE/Server-Features: New PIN-Modus, Next Token-Modus, DES/SDI-Verschlüsselung, AES-Verschlüsselung, Unterstützung untergeordneter ACE/Server, Namenssperrungen und Clustering. Das IVE unterstützt über das RADIUS-Protokoll auch die New PIN- und Next Token-Modi von RSA SecurID.

Hinweis: Wegen der Einschränkungen der ACE/Server-Bibliothek unter UNIX können Sie u.U. nur eine ACE/Server-Konfiguration festlegen. Informationen zum Erzeugen einer ACE/Agent-Konfigurationsdatei für die IVE-Appliance auf dem ACE-Server finden Sie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 219.

☑ Definieren einer ACE/Serverinstanz

Hinweis: Sie können nur eine ACE/Serverinstanz hinzufügen.

So definieren Sie einen ACE/Server:

1. Erzeugen Sie eine ACE/Agent-Konfigurationsdatei (`sdconf.rec`) für das IVE auf dem ACE-Server (Seite 219).
2. Wählen Sie in der Web console **System > Signing In > Servers** aus.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **ACE Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
4. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.

Hinweis: Wenn die Endbenutzer SecurID-Softwaretokens an ACE/Server übergeben, können Sie die Verwendung von Leerzeichen oder anderen nicht alphanumerischen Zeichen im Namen der Serverinstanz vermeiden. Um SecurID-Softwaretokenwerte transparent an ACE/Server zu übergeben, müssen Benutzer anhand des folgenden URLs zur Seite „RSA SecurID Authentication“ wechseln: **https://IVE/login/ServerInstanz** (wobei „IVE“ die IP-Adresse oder den Hostnamen der IVE appliance und „ServerInstanz“ den oben festgelegten Namen darstellt). Wenn der Name der Serverinstanz Leerzeichen oder andere nicht alphanumerische Zeichen enthält, muss der Benutzer Escapezeichen (z.B. %20) in den URL einfügen.

---

5. Geben Sie im Feld **ACE Port** einen Standardport an. Das IVE verwendet diese Einstellung nur, wenn in der Datei `sdconf.rec` kein Port angegeben ist.
6. Importieren Sie die RSA ACE/Agent-Konfigurationsdatei. Aktualisieren Sie diese Datei im IVE unbedingt bei jeder Änderung an der Quelldatei. Ebenso müssen Sie, wenn Sie die Instanzdatei aus dem IVE löschen, zur Konfigurationsverwaltungsanwendung für ACE-Server wechseln, wie unter „Generieren einer ACE/Agent-Konfigurationsdatei“ auf Seite 219 beschrieben, und das Kontrollkästchen **Sent Node Secret** deaktivieren.
7. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
8. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.

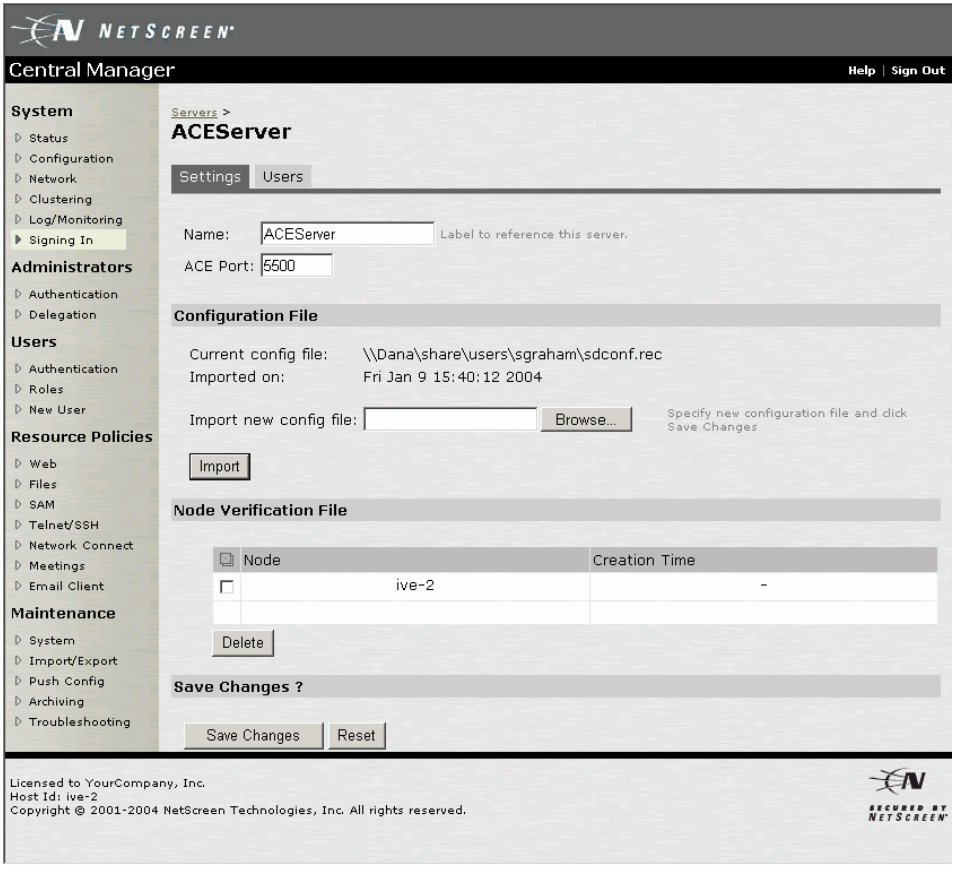


Abbildung 54: System > Signing In > Servers > ACE Server

☑ Generieren einer ACE/Agent-Konfigurationsdatei

Wenn Sie ACE/Server für die Authentifizierung verwenden, müssen Sie auf dem ACE-Server eine ACE/Agent-Konfigurationsdatei (`sdconf.rec`) für das IVE generieren.

So generieren Sie eine ACE/Agent-Konfigurationsdatei:

1. Starten Sie die Konfigurationsverwaltungsanwendung für ACE-Server, und klicken Sie auf **Agent Host**.
2. Klicken Sie auf **Add Agent Host**.
3. Geben Sie unter **Name** einen Namen für den IVE-Agent ein.
4. Geben Sie unter **Network Address** die IP-Adresse des IVE ein.
5. Geben Sie eine auf dem ACE-Server konfigurierte **Site** an.
6. Wählen Sie als **Agent Type** den Typ **Communication Server** aus.
7. Wählen Sie als **Encryption Type** den Typ **DES** aus.
8. Vergewissern Sie sich, dass **Sent Node Secret** (beim Erstellen eines neuen Agents) deaktiviert ist.

   Wenn der ACE-Server eine vom IVE gesendete Anforderung erfolgreich authentifiziert, wählt der ACE-Server **Sent Node Secret** aus. Wenn der ACE-Server später einen neuen Knotenschlüssel an das IVE senden soll, gehen Sie bei der nächsten Authentifizierungsanforderung folgendermaßen vor:

   1. Deaktivieren Sie das Kontrollkästchen **Sent Node Secret**, indem Sie auf dieses klicken.
   2. Melden Sie sich an der Web console des IVE an, und wählen Sie **System > Signing In > Servers** aus.
   3. Klicken Sie in der Liste **Authentication/Authorization Servers** auf den Namen des entsprechenden ACE-Servers.
   4. Aktivieren Sie unter **Node Verification File** das entsprechende Kontrollkästchen aus, und klicken Sie auf **Delete**. Durch diese Schritte wird sichergestellt, dass der IVE-Server und der ACE-Server synchronisiert sind. Entsprechend sollten Sie auf dem ACE-Server das Kontrollkästchen **Sent Node Secret** deaktivieren, wenn Sie die Überprüfungsdatei aus dem IVE löschen.
9. Klicken Sie auf **Assign Acting Servers**, und wählen Sie den ACE-Server aus.
10. Klicken Sie auf **Generate Config File**. Wenn Sie den ACE-Server zum IVE hinzufügen, wird diese Konfigurationsdatei importiert.

Konfigurieren einer Active Directory- oder einer NT-Domäneninstanz

Wenn die Benutzerauthentifizierung über einen primären NT-Domänencontroller oder Active Directory erfolgt, melden sich Benutzer am IVE mit dem Benutzernamen und dem Kennwort an, mit denen sie auf den eigenen Windows-Desktop zugreifen.

☑ Definieren einer Active Directory- oder Windows NT-Domänenserverinstanz

So definieren Sie einen Active Directory- oder Windows NT-Domänenserver:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Active Directory/ Windows NT** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des primären Domänencontrollers oder von Active Directory an.
5. Geben Sie die IP-Adresse des Sicherungsdomänencontrollers oder von Active Directory an. (Optional.)
6. Geben Sie den Domänennamen für die Benutzer ein, denen Sie den Zugriff gewähren möchten.
7. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
8. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.

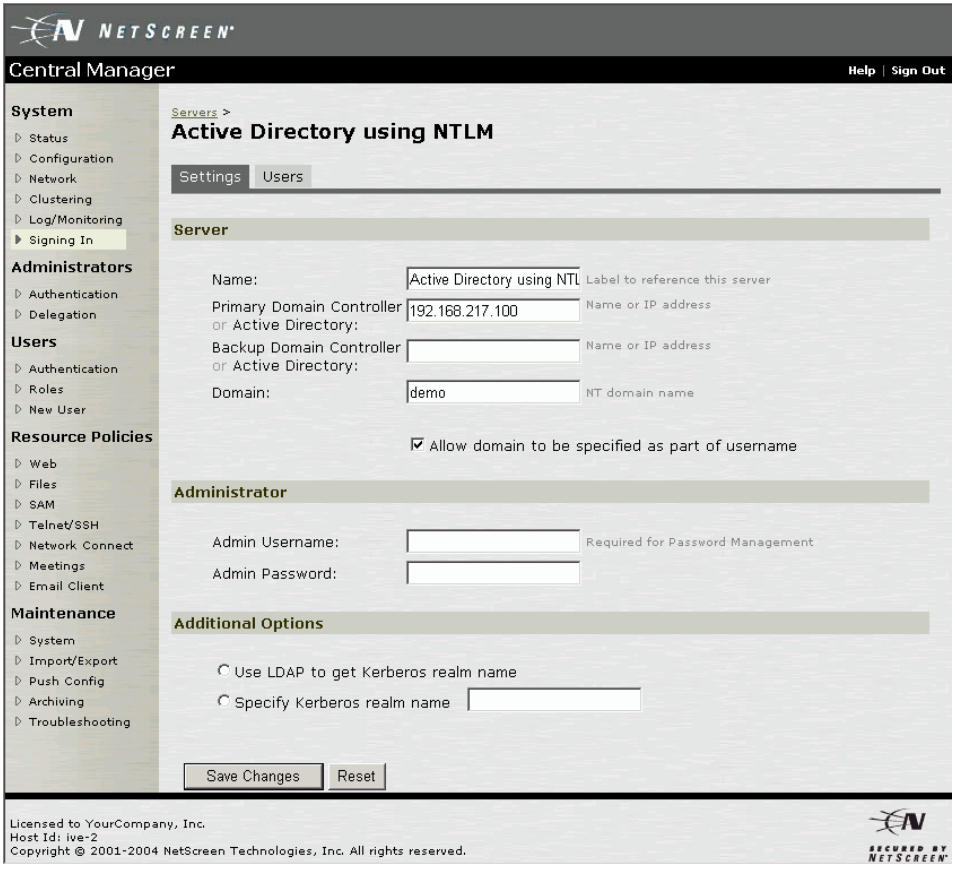


Abbildung 55: System > Signing In > Servers > Active Directory/Windows NT

Konfigurieren einer Instanz eines anonymen Servers

Ein anonymer Server ermöglicht Benutzern den Zugriff auf das IVE ohne Angabe von Benutzername oder Kennwort. Wenn ein Benutzer den URL einer Anmeldeseite eingibt, für die Authentifizierung durch einen anonymen Server konfiguriert ist, umgeht das IVE die IVE-Standardanmeldeseite und zeigt dem Benutzer sofort die IVE-Willkommensseite an.

Sie können anonyme Authentifizierung auswählen, wenn Sie es nicht für notwendig halten, dass die Ressourcen auf dem IVE sehr hohen Sicherheitsanforderungen unterliegen oder wenn Sie die anderen Sicherheitsmaßnahmen auf dem IVE für ausreichend halten. Sie können z.B. eine Benutzerrolle mit beschränktem Zugriff auf interne Ressourcen erstellen und diese Rolle dann mithilfe einer Richtlinie authentifizieren, die nur verlangt, dass sich Benutzer von einer IP-Adresse aus Ihrem internen Netzwerk anmelden. Bei dieser Methode wird davon ausgegangen, dass ein Benutzer, der zum Zugriff auf das interne Netzwerk berechtigt ist, auch die Ressourcen anzeigen darf, die im Rahmen dieser Benutzerrolle bereitgestellt werden.

Beachten Sie bei der Definition und Überwachung einer Instanz eines anonymen Servers Folgendes:

- Sie können nur eine Konfiguration für anonyme Server hinzufügen.
- Administratoren können nicht mithilfe eines anonymen Servers authentifiziert werden.

9. Bei der Konfiguration müssen Sie auf der Registerkarte **Users > Authentication** > **General** den anonymen Server als Authentifizierungsserver und als Verzeichnis-/Attributserver auswählen (Seite 273).

- Beim Erstellen von Rollenzuordnungsregeln auf der Registerkarte **Users > Authentication** > **Role Mapping** (Seite 277) gestattet das IVE keine Erstellung von Zuordnungsregeln, die für bestimmte Benutzer gelten (z.B. „Joe"), da auf einem anonymen Server keine Informationen zu Benutzernamen gespeichert werden. Sie können Rollenzuordnungsregeln erstellen, die auf einem Standardbenutzernamen (*), Zertifikatattributen oder benutzerdefinierten Ausdrücken basieren.
- Aus Sicherheitsgründen können Sie ggf. die Anzahl der Benutzer beschränken, die sich gleichzeitig über einen anonymen Server anmelden. Verwenden Sie dazu die Option auf der Registerkarte **Users > Authentication > [Bereich] > Authentication Policy > Limits**. Dabei ist **[Bereich]** der Bereich, für Benutzerauthentifizierung durch den anonymen Server konfiguriert ist (Seite 275).

- Sie können die Sitzungen von anonymen Benutzern (im Gegensatz zu anderen Authentifizierungsservern) nicht löschen und nicht über die Registerkarte **Users** anzeigen, da keine Benutzernamen eingegeben wurden und das IVE daher keine individuellen Sitzungsdaten anzeigen kann.

☑ Definieren einer Instanz eines anonymen Servers

So definieren Sie einen anonymen Server:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **Anonymous Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Klicken Sie auf **Save Changes**.
5. Geben Sie die Bereiche an, die der Server für die Autorisierung von Benutzern verwenden soll (Seite 273).

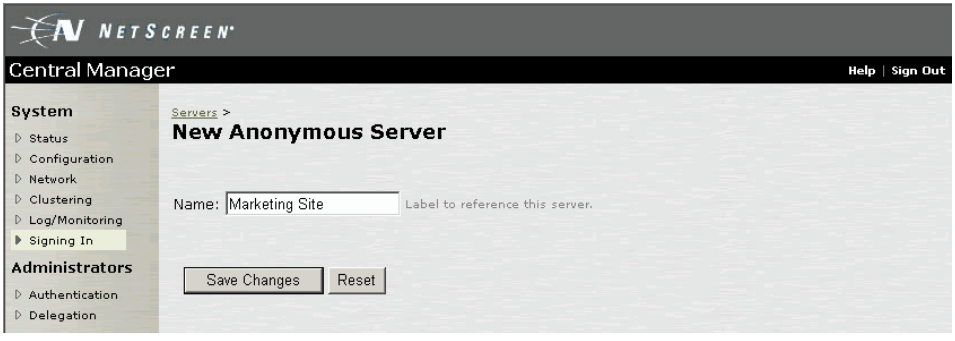


Abbildung 56: System > Signing In > Servers > Anonymous Server

Konfigurieren einer Zertifikatserverinstanz

Der Zertifikatserver ermöglicht die Authentifizierung von Benutzern anhand von Attributen in clientseitigen Zertifikaten. Sie können den Zertifikatserver allein oder in Verbindung mit einem anderen Server verwenden, um Benutzer zu authentifizieren und sie Rollen zuzuordnen.

Sie könnten Benutzer z.B. allein anhand ihrer Zertifikatattribute authentifizieren. Wenn das IVE ein Benutzerzertifikat als gültig einstuft, wird der Benutzer auf der Grundlage seines CN (Common Name) angemeldet, der im Zertifikat enthalten ist. Der Benutzer muss keinen Benutzernamen und kein Kennwort angeben.

Sie können Benutzer auch authentifizieren, indem Sie ihre Clientzertifikatattribute an einen zweiten Authentifizierungsserver (wie LDAP) weiterleiten. In diesem Szenario ermittelt der Zertifikatserver zunächst, ob das Benutzerzertifikat gültig ist. Wenn dies der Fall ist, leitet der Zertifikatserver ausgewählte Attribute an einen LDAP-Server mit einer CRL (Certificate Revocation List, Zertifikatssperrliste) weiter. Wenn das Zertifikat des Benutzers gesperrt wurde (weil er beispielsweise nicht mehr in der Firma tätig ist oder seine berufliche Position gewechselt hat), gibt der LDAP-Server den Status „unzulässig" an das IVE zurück und dieser verweigert dem Benutzer den Zugriff. Wenn der LDAP-Server den Zustand „zulässig" zurückgibt, wird der Benutzer vom IVE einer Rolle zugewiesen, die auf einem vom LDAP-Server zurückgegebenen Wert basiert.

Bei der Authentifizierung von Benutzern anhand ihrer Zertifikatattribute empfiehlt es sich, die Benutzer anzuweisen, ihre Browser nach Beenden ihrer IVE-Sitzungen zu schließen. Dies gewährleistet, dass auf den Benutzersystemen keine Client-Anmeldeinformationen (wie Cookies und Zertifikate) zwischengespeichert werden.

☑ Festlegen einer Zertifikatserverkonfiguration

Gehen Sie zum Festlegen eines Zertifikatservers auf dem IVE folgendermaßen vor:

1. Importieren Sie die Stammzertifizierungsstelle, mit der die Clientzertifikate signiert werden:
   1. Navigieren Sie zu **System > Configuration > Certificates > CA Certificates**.
   2. Importieren Sie das Stammzertifikat.

2. Konfigurieren Sie eine Zertifikatserverinstanz:
   1. Navigieren Sie zu **System > Signing In > Servers**.
   2. Wählen Sie aus der Liste **New** den Eintrag **Certificate Server** aus, und klicken Sie anschließend auf **New Server**.
   3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen. Wenn Sie den Namen eines vorhandenen Servers ändern, erstellt das IVE eine neue Zertifikatinstanz mit dem neuen Namen und behält den alten Server jedoch weiterhin.
   4. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.

   Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die gegenwärtig über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.
3. Erstellen Sie eine LDAP-Serverinstanz, sofern Zertifikatattribute mit LDAP überprüft werden sollen (optional). Zum Abrufen der benutzerspezifischen Attribute, die durch das Zertifikat überprüft werden sollen, müssen Sie die Optionen **Finding user entries** auf der LDAP-Konfigurationsseite verwenden .
4. Erstellen Sie einen Authentifizierungsbereich über eine der folgenden Registerkarten:
   - **Users > Authentication**
   - **Administrators > Authentication**
5. Konfigurieren Sie den Bereich für den bzw. die neuen Server:
   1. Navigieren Sie zu **Users/Administrators > Authentication > General**.
   2. Wählen Sie den Zertifikatserver aus der Liste **Authentication Server** aus.
   3. Wählen Sie in der Liste **Directory/Attribute server** den LDAP-Server (sofern vorhanden) oder **None** aus.
6. Wenn der Benutzerzugriff auf den Bereich anhand einzelner Zertifikatattribute eingeschränkt werden soll:
   1. Navigieren Sie zu **Users/Administrators > Authentication > [Bereich] > Authentication Policy > Certificate**.
   2. Wählen Sie die Option **Only allow users with client-side certificate...** aus.
   3. Geben Sie an, welche Werte das Benutzer-/Administratorzertifikat enthalten muss.

7. Wenn Benutzer anhand einzelner Zertifikatattribute zu Rollen zugeordnet werden sollen:
   1. Navigieren Sie zu **Users/Administrators > Authentication > [Bereich] > Role Mapping**.
   2. Wählen Sie **New Rule** und dann **Certificate** aus der Liste **Rule based on** aus, und klicken Sie dann auf **Update**, um Optionen zum Erstellen einer zertifikatbasierten Regel anzuzeigen.
   3. Geben Sie eine Rollenzuordnungsregel auf der Grundlage des Zertifikatattributs ein. Zu allgemeinen Zertifikatattributen gehören:
      - CN: Common Name (engl. für üblicher Name). Enthält häufig den Benutzernamen.
      - OU: Organizational Unit (engl. für Organisationseinheit). Enthält den Firmennamen des Benutzers.
8. Konfigurieren Sie mithilfe von benutzerdefinierten Ausdrücken komplexere Regeln, die auf Zertifikatattributen beruhen (optional).

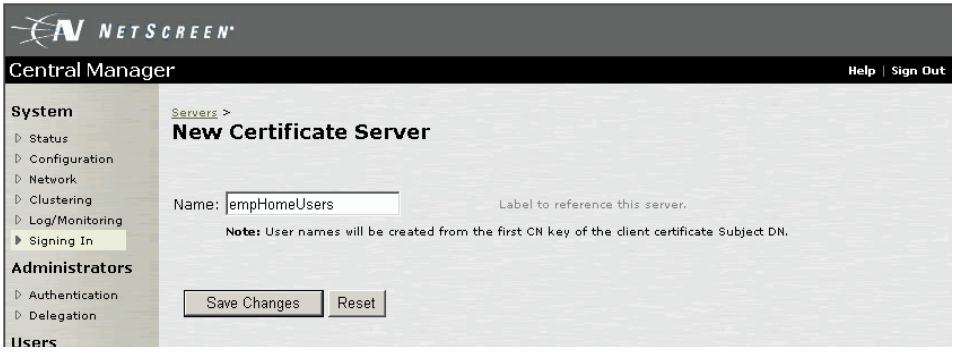


Abbildung 57: System > Signing In > Servers > Certificate Server

Konfigurieren einer LDAP-Serverinstanz

Das IVE unterstützt zwei LDAP-spezifische Authentifizierungsoptionen:

- **Unencrypted** – Benutzername und Kennwort werden im Klartext (unverschlüsselt) an den LDAP-Verzeichnisdienst gesendet.
- **LDAPS** – Die Daten in der LDAP-Authentifizierungssitzung werden mit dem SSL-Protokoll (Secure Socket Layer) verschlüsselt, bevor sie an den LDAP-Verzeichnisdienst gesendet werden.

Das IVE unterstützt außerdem dynamische LDAP-Gruppen und LDAP-Kennwortverwaltung über das IVE. Mithilfe der Kennwortverwaltung können Benutzer, die sich über einen LDAP-Server authentifizieren, ihre Kennwörter anhand der auf dem LDAP-Server definierten Richtlinien über das IVE zu verwalten[1]. Beispiel: Ein Benutzer verwendet für die Anmeldung am IVE ein Kennwort, dessen Gültigkeit in Kürze abläuft. Das IVE fängt die Benachrichtigung über das abgelaufene Kennwort ab, zeigt sie dem Benutzer in der IVE-Oberfläche an und leitet dann die Antwort des Benutzers an den LDAP-Server zurück, ohne dass sich der Benutzer separat am LDAP-Server anmelden muss.

Weitere Informationen finden Sie unter:

Definieren einer LDAP-Serverinstanz 229
Unterstützte Funktionen für die LDAP-Kennwortverwaltung 232

☑ Definieren einer LDAP-Serverinstanz

So definieren Sie eine LDAP-Serverinstanz:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **LDAP Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des LDAP-Servers an, der vom IVE zur Überprüfung von Benutzern verwendet wird.

1. Die LDAP-Kennwortverwaltung ist eine lizenzierte Funktion.

5. Geben Sie den Port an, den der LDAP-Server überwacht. Dies ist bei Verwendung einer unverschlüsselten Verbindung normalerweise Port 389 und bei Verwendung von SSL Port 636.
6. Geben Sie Parameter für LDAP-Sicherungsserver an (optional). Das IVE verwendet die angegebenen Server für die Failover-Verarbeitung. Jede Authentifizierungsanforderung wird zunächst an den primären LDAP-Server weitergeleitet und dann an den oder die angegebenen Sicherungsserver, falls der primäre Server nicht erreichbar ist.

   Hinweis: LDAP-Sicherungsserver müssen dieselbe Version wie der primäre LDAP-Server aufweisen. Beim Angeben von LDAP-Sicherungsservern empfiehlt es sich, nicht den Hostnamen, sondern die IP-Adresse anzugeben. Dies kann die Failover-Verarbeitung beschleunigen, da der Hostname nicht in eine IP-Adresse aufgelöst werden muss.

7. Geben Sie an, ob die Verbindung zwischen dem IVE und dem LDAP-Verzeichnisdienst unverschlüsselt bleiben oder ob SSL (LDAPs) verwendet werden soll.
8. Geben Sie den Typ des LDAP-Servers an, über den Sie Benutzer authentifizieren möchten. Das IVE unterstützt dynamische Gruppen mit Active Directory und iPlanet-Servern.
9. Klicken Sie auf **Test Connection**, um die Verbindung zwischen der IVE appliance und den angegebenen LDAP-Servern zu prüfen. (optional) Das IVE kann Verbindungen mit dem primären Server und beiden Sicherungsservern testen.
10. Wenn das IVE gegen das LDAP-Verzeichnis authentifiziert werden soll, um eine Suche durchzuführen oder das Kennwort mithilfe der Kennwortverwaltungsfunktion zu ändern (Seite 232), aktivieren Sie das Kontrollkästchen **Authentication required to search LDAP**, und geben Sie Administrator-DN und -Kennwort ein.

    Beispiel:
    `DN: CN=Administrator, CN=Users, DC=eng, DC=NetScreen, DC=com`

    Hinweis: Dies ist erforderlich, wenn Kennwörter in Active Directory geändert oder ein Dynamic DN zum Durchsuchen der Active Directory-Datenbank verwendet werden soll.

11. Geben Sie unter **Finding user entries** Folgendes an:
    - **Base DN**, von dem an nach Benutzereinträgen gesucht werden soll.
    - **Filter**, wenn die Suche eingegrenzt werden soll. Hinweis:
      - Fügen Sie zur Verwendung des Benutzernamens, der auf der Anmeldeseite für die Suche eingegeben wird, im Filter die Zeichenfolge `<USER>` (in Großbuchstaben) ein.

        Beispiel: `DN: CN=cay, CN=dave, ou=eng, ou=mktg, o=netscreen.com`

- Es empfiehlt sich, einen Filter anzugeben, der keinen oder einen Benutzer-DN zurückgibt.

12. Geben Sie unter **Determining group membership** Folgendes an:
    - **Base DN**, von dem an nach Benutzereinträgen gesucht werden soll.
    - **Filter**, wenn die Suche eingegrenzt werden soll.
    - **Member Attribute**, um die Mitglieder einer statischen Gruppe anzugeben.
    - **Query Attribute**, um die Mitglieder einer dynamischen Gruppe anzugeben.
13. Wählen Sie unter **Bind Options** Folgendes aus:
    - **Simple bind**, um Daten im Klartext (unverschlüsselt) an den LDAP-Verzeichnisdienst zu senden.
    - **StartTLS bind**, um die Daten in der LDAP-Authentifizierungssitzung über das TLS-Protokoll (Transport Layer Security) zu verschlüsseln, bevor sie an den LDAP-Verzeichnisdienst gesendet werden.
14. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
15. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.

Unterstützte Funktionen für die LDAP-Kennwortverwaltung

Im Folgenden werden die LDAP-Kennwortrichtlinie sowie die Sperr- und Validierungsfunktionen beschrieben, die das IVE bei der Authentifizierung mit LDAP-Servern für Microsoft Active Directory, Sun iPlanet und Novell eDirectory unterstützt. (Bei der Authentifizierung mit einem generischen LDAP-Server wie IBM Secure Directory unterstützt das IVE nur die Authentifizierung und erlaubt es dem Benutzer, sein Kennwort zu ändern.) Diese Funktionen müssen durch den LDAP-Server selbst festgelegt werden, bevor das IVE die entsprechenden Meldungen, Funktionen und Beschränkungen an Endbenutzer weitergeben kann.

Hinweis: Beim Verwenden von Active Directory müssen Sie Folgendes beachten:
– In Active Directory kann das Aktualisieren einer Richtlinie bis zu 90 Minuten dauern, wenn Richtlinienfunktionen festgelegt werden. Bis Active Directory die Aktualisierung einer Richtlinie abgeschlossen hat, bleiben die alten Richtlinieneinstellungen in Kraft.
– Um das Ändern von Kennwörtern beim Verwenden der Active Directory-Kennwortverwaltung zu unterstützen, muss LDAPS auf dem Active Directory-Server aktiviert sein. Das ist genauso einfach wie das Importieren eines gültigen signierten SSL-Zertifikats in den Personal Certificates Store (mit der MMC bei Auswahl des Certificates-Snap-In verfügbar). Das CN-Subjekt dieses Zertifikats muss genau mit dem Hostnamen des Active Directory-Servers übereinstimmen. Das SSL-Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle signiert sein, einschließlich vertrauenswürdigen lokalen Zertifizierungsstellen. Beachten Sie, dass das Stammzertifikat in einem Stammzertifikatspeicher installiert sein muss, damit eine Vertrauensbeziehung hergestellt werden kann.

Unterstützte Funktionen für Kennwortrichtlinien:

- Authentifizieren des IVE-Benutzers durch den LDAP-Server.
- Dem Benutzer gestatten, sein LDAP-Kennwort auf der IVE-Seite **System > Preferences** zu ändern.
- Abmelden des Benutzers vom IVE nach erfolgreicher Änderung des LDAP-Kennwortes.
- Festlegen, dass der Benutzer sein LDAP-Kennwort bei der nächsten Annmeldung am IVE ändern muss.

Hinweis: Wenn Sie diese Option für einen iPlanet-Server aktivieren, müssen Sie beachten, dass Sie sich anschließend am Directory Manager anmelden und das Kennwort des Benutzers ändern müssen, um den Benutzer zurückzusetzen. Bei der nächsten Anmeldung des Benutzers mit dem neuen Kennwort, wird der Benutzer vom IVE zum Ändern seines Kennwortes aufgefordert.

- Benachrichtigen des Benutzers über den Ablauf des LDAP-Kennwortes.
- Den Benutzer 14 Tage im Voraus vom Ablauf seines LDAP-Kennwortes informieren.

Hinweis: Beim Aktivieren dieser Option auf einem der folgenden Sever:
– iPlanet-Server. Beachten Sie, dass das IVE nur Richtlinien für das Ablaufen von Kennwörtern auf Benutzerebene erkennt, keine Richtlinien auf Gruppenebene.
– Active Directory-Server. Beachten Sie, dass das Kontoablaufdatum keinen Einfluss auf das Ablaufdatum des Benutzerkennwortes hat.

Unterstützte Funktionen für die Kennwortsperrung:

- Sperren des Zugriffs auf das IVE und den LDAP-Server, wenn das Kennwort des Benutzers deaktiviert oder gesperrt ist.

Unterstützte Funktionen für die Kennwortvalidierung:

- Erzwingen einer Mindestlänge für LDAP-Kennwörter.
- Erzwingen eines Mindestalters für LDAP-Kennwörter, um zu verhindern, dass der Benutzer sein Kennwort zu häufig ändert.
- Festlegen einer Komplexitätsanforderung für LDAP-Kennwörter, um zu verhindern, dass der Benutzer seinen Benutzernamen, seinen Vornamen oder seinen Nachnamen im Kennwort verwendet. Außerdem soll das Kennwort 3 Zeichen aus den folgenden Kategorien enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen (beispielsweise !, $, %).
- Berücksichtigen der LDAP-Kennworthistorie des Benutzers.

Wenn Sie den Wert für die Kennworthistorie auf null festlegen, kann der Benutzer dasselbe Kennwort erneut verwenden.

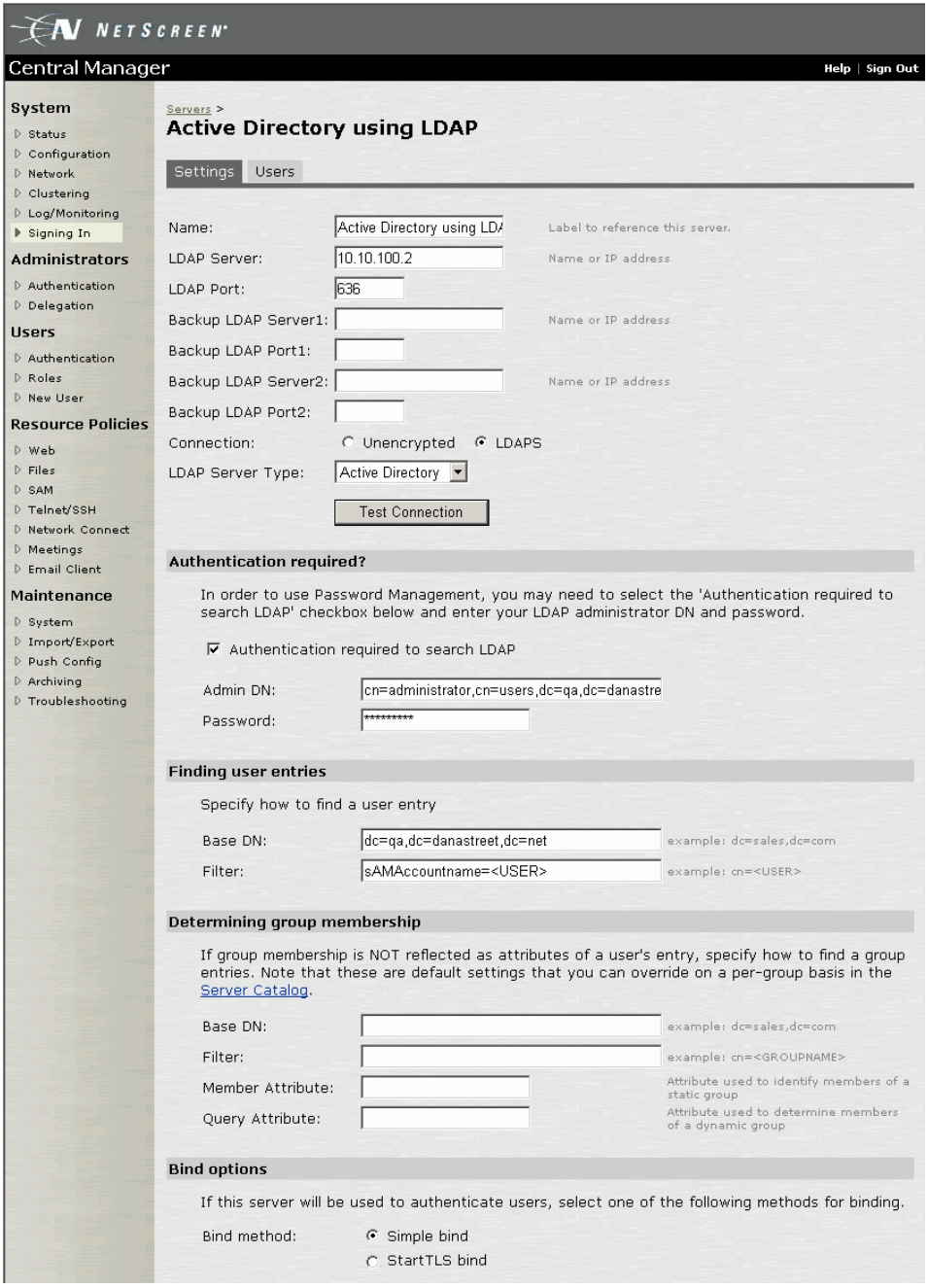


Abbildung 58: System > Signing In > Servers > LDAP Server

Konfigurieren einer lokalen IVE-Server-Instanz

Im IVE können Sie eine oder mehrere lokale Datenbanken für vom IVE authentifizierte Benutzer erstellen. Sie können lokale Benutzerdatensätze für Benutzer erstellen, die normalerweise von einem externen Authentifizierungsserver überprüft werden, der deaktiviert werden soll. Dies bietet sich auch an, wenn Sie eine Gruppe von temporären Benutzern erstellen möchten. Hinweis: Alle Administratorenkonten werden als lokale Datensätze gespeichert, Administratoren können jedoch über einen externen Server authentifiziert werden. Anweisungen hierfür finden Sie unter „Angeben einer Richtlinie für einen Authentifizierungsbereich“ auf Seite 275.

In diesem Abschnitt werden folgende Vorgänge behandelt:

Definieren einer lokalen IVE-Server-Instanz 235
Erstellen lokaler Benutzer 236
Verwalten von Benutzerkonten..... 237
Delegieren von Benutzerverwaltungsrechten an Endbenutzer 238

☑ Definieren einer lokalen IVE-Server-Instanz

So definieren Sie einen lokalen IVE-Server:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **IVE Authentication** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Users** und **Admin Users** angezeigt.
5. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 275).

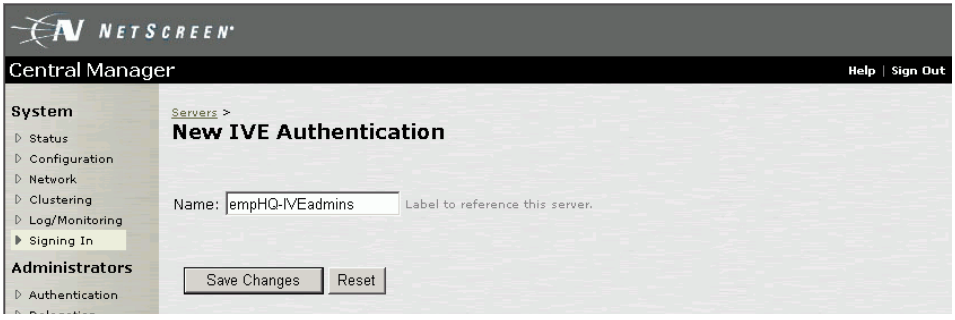


Abbildung 59: System > Signing In > Servers > Local IVE Authentication

☑ Erstellen lokaler Benutzer

Wenn Sie als Typ des Authentifizierungsservers „IVE Authentication" auswählen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Ein Datensatz für einen lokalen Benutzer besteht aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Datensätze für lokale Benutzer können für Benutzer erstellt werden, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung:

1. Führen Sie in der Web console einen der folgenden Vorgänge aus:
   - Wählen Sie **System > Signing In > Servers** aus, und klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten. Klicken Sie auf die Registerkarte **Users** und dann auf **New**.
   - Wählen Sie **Users > New User** aus.
2. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein. Hinweis:
   - In Benutzernamen darf die Zeichenkombination „~~" nicht enthalten sein.
   - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
3. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

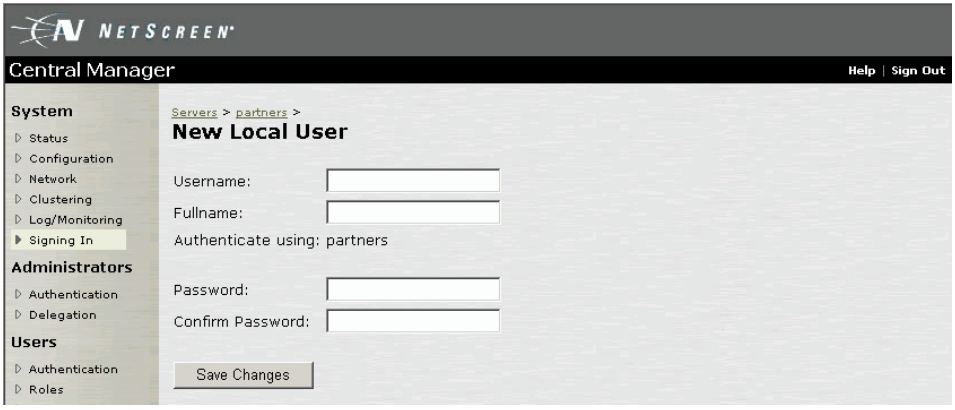


Abbildung 60: Users > Signing In > Servers > Local IVE Authentication > Users > New User

☑ Verwalten von Benutzerkonten

Die Konfigurationsseite für lokale IVE-Authentifizierungsserver enthält eine Registerkarte **Users**, auf der Sie aktive IVE-Benutzerkonten anzeigen, bearbeiten und löschen können.

So verwalten Sie ein lokales Benutzerkonto:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Verknüpfung.
3. Klicken Sie auf die Registerkarte **Users**.
4. Führen Sie eine der folgenden Aufgaben durch:
   - Geben Sie im Feld **Show Users Named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (`*`) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z.B. nach allen Benutzernamen suchen möchten, die die Buchstaben `jo` enthalten, geben Sie im Feld **Show users named** die Zeichenfolge `*jo*` ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die Gesamtliste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (`*`) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.

- Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.
- Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

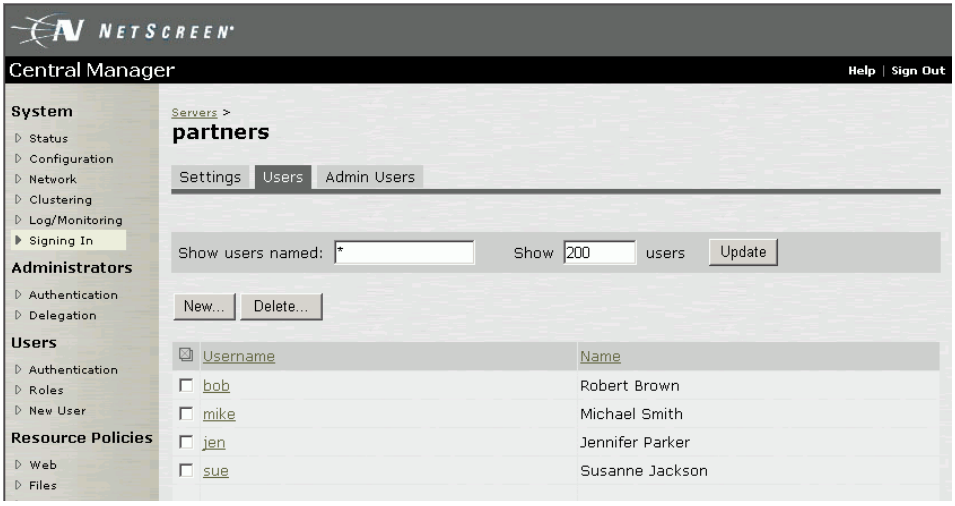


Abbildung 61: System > Signing In > Servers > Local IVE Authentication > Users

☑ Delegieren von Benutzerverwaltungsrechten an Endbenutzer

Auf der Registerkarte **System > Signing In > Admin Users** können Sie Benutzerverwaltungsrechte an ausgewählte Endbenutzer delegieren, einschließlich des Rechts, Benutzer zu einem lokalen IVE-Authentifizierungsserver hinzuzufügen, Benutzer zu löschen, vollständige Namen von Benutzern zu bearbeiten und Benutzerkennwörter über das Menü **User Admin** auf der Startseite des sicheren Gateways zu ändern.

Hinweis: Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten. Außerdem dürfen Benutzeradministratoren keine Bereiche oder Rollenzuordnungen verwalten. Daher wird die Aktivierung der Funktion „User Admin“ nur dann empfohlen, wenn die Rollenzuordnungsregeln des Authentifizierungsbereichs es nicht zugeordneten Benutzern (*) erlauben, sich am IVE anzumelden, sodass der Benutzeradministrator neue Benutzer ohne Eingreifen des Administrators hinzufügen kann. (Wenn die Rollenzuordnungen automatisch erfolgen, können Benutzeradministratoren die neuen Benutzer ohne Hilfe des Administrators manuell einer Rolle zuordnen.)

So delegieren Sie Benutzerverwaltungsrechte an einen Endbenutzer:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Wählen Sie die lokale IVE-Authentifizierungsserver-Instanz aus, die vom Benutzeradministrator verwaltet werden soll, und klicken Sie dann auf die Registerkarte **Admin Users**.

   Hinweis: Benutzeradministratoren können nur lokale IVE-Authentifizierungsserver verwalten.

3. Geben Sie den **Username** des Benutzers ein, der Konten für den ausgewählten Authentifizierungsserver verwalten soll. (Der ausgewählte Benutzer muss auf dem Server, den er verwaltet, nicht als lokaler Benutzer hinzugefügt werden.)

   Hinweis: Achten Sie bei der Eingabe des Benutzernamens des Benutzeradministrators auf die exakte Zeichenfolge. Diese muss genau übereinstimmen.

4. Wählen Sie den **Authentication Realm** aus, dem der Benutzeradministrator zugeordnet wird, wenn er sich am IVE anmeldet.
5. Klicken Sie auf **Add**. Das IVE fügt den neuen Benutzeradministrator der Liste **User Admins** im folgenden Format hinzu: `Benutzername@Servername`.
6. Wenn der angegebene Benutzeradministrator mehreren Bereichen zugeordnet ist, wiederholen Sie ggf. die Schritte 3 bis 5, sodass der Benutzer den Server unabhängig von dem Konto verwalten kann, über das er sich beim IVE anmeldet.
7. Um dem Benutzer die Verwaltungsrechte wieder zu entziehen, wählen Sie in der Liste **User Admins** den entsprechenden Namen aus, und klicken Sie auf **Remove**.

Hinweis: Informationen zum Verwalten von Benutzern über die Startseite des sicheren Gateways finden Sie in der Hilfe zum sicheren Gateway im Thema „Hinzufügen, Ändern und Löschen von Benutzern“, d.h. in der über das IVE verfügbaren Benutzerhilfe.

Konfigurieren einer NIS-Serverinstanz

Beim Authentifizieren von Benutzern mit einem UNIX/NIS-Server überprüft der IVE, ob der auf der Anmeldeseite eingegebene Benutzername und das Kennwort einem gültigen Paar aus Benutzer-ID und Kennwort auf dem NIS-Server entsprechen. Beachten Sie, dass der an das IVE gesendete Benutzername keine zwei aufeinander folgenden Tilden (~~) enthalten darf.

Hinweis: Sie können NIS-Authentifizierung nur mit dem IVE verwenden, wenn die Kennwörter auf dem NIS-Server im Crypt- oder MD5-Format gespeichert sind. Außerdem können Sie dem IVE nur eine NIS-Serverkonfiguration hinzufügen, mit der jedoch eine beliebige Anzahl von Bereichen authentifiziert werden können.

☑ Festlegen einer NIS-Serverinstanz

So definieren Sie eine NIS-Serverinstanz:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **NIS Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des NIS-Servers an.
5. Geben Sie den Domänennamen für den NIS-Server an.
6. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
7. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.

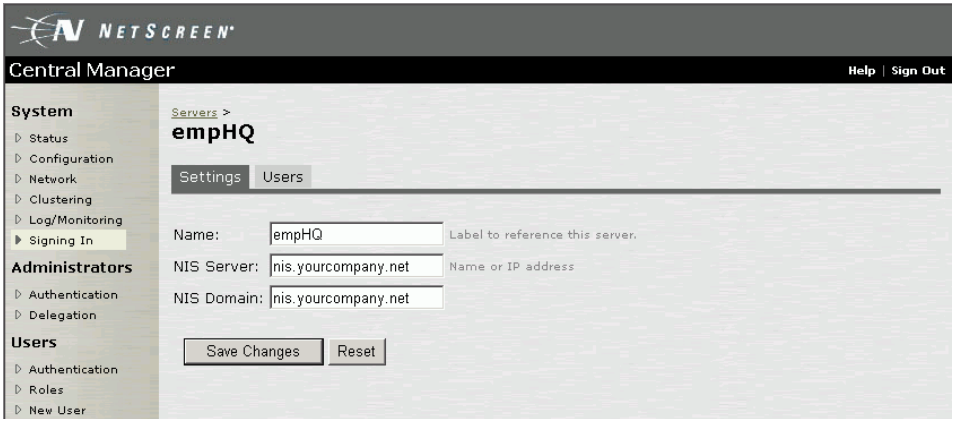


Abbildung 62: System > Signing In > Servers > NIS Server

Konfigurieren einer RADIUS-Serverinstanz

Für die Benutzerauthentifizierung mit einem RADIUS-Server müssen Sie diesen so konfigurieren, dass das IVE als Client erkannt wird. Außerdem müssen Sie für den RADIUS-Server einen gemeinsamen geheimen Schlüssel angeben, der für die Authentifizierung der Clientanforderung verwendet wird.

Das IVE unterstützt die RADIUS-Standardauthentifizierungsschemas. Diese lauten: Access-Request, Access-Accept, Access-Reject und Access-Challenge. Der IVE unterstützt auch RSA ACE/Server unter Verwendung des RADIUS-Protokolls und eines SecurID-Tokens (erhältlich von Security Dynamics). Wenn Sie für die Authentifizierung von Benutzern SecurID verwenden, müssen die Benutzer ihre Benutzer-ID und die Kombination aus PIN und dem Tokenwert angeben.

Wenn Sie einen PassGo Defender-RADIUS-Server verwenden, erfolgt die Benutzeranmeldung folgendermaßen:

1. Der Benutzer meldet sich beim IVE mit einem Benutzernamen und einem Kennwort an. Das IVE leitet diese Anmeldeinformationen an Defender weiter.
2. Defender sendet eine eindeutige Anfragezeichenfolge an das IVE, und im IVE wird diese Anfragezeichenfolge dem Benutzer angezeigt.
3. Der Benutzer gibt die Anfragezeichenfolge in einem Defender-Token ein, und das Token erzeugt eine Antwortzeichenfolge.
4. Der Benutzer gibt die Antwortzeichenfolge im IVE ein und klickt auf **Sign In**.

☑ Definieren eines RADIUS-Servers

So definieren Sie einen RADIUS-Server:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie in der Liste **New** den Eintrag **Radius Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
3. Geben Sie einen Namen ein, um die Serverinstanz zu bezeichnen.
4. Geben Sie den Namen oder die IP-Adresse des RADIUS-Servers an.

5. Geben Sie den Port für den RADIUS-Server ein. Normalerweise ist dies Port 1645.
6. Geben Sie eine Zeichenfolge für den gemeinsamen geheimen Schlüssel ein. Sie müssen diese Zeichenfolge auch eingeben, wenn Sie den RADIUS-Server für die Erkennung des IVE-Geräts als Client konfigurieren.
7. Geben Sie die Zeitspanne ein, für die das IVE auf eine Antwort vom RADIUS-Server bis zur Zeitüberschreitung für die Verbindung warten soll.
8. Geben Sie die Anzahl der weiteren Verbindungsversuche ein, die das IVE nach dem ersten fehlgeschlagenen Versuch ausführen soll.
9. Geben Sie einen sekundären RADIUS-Server an, der vom IVE verwendet wird, wenn der primäre, in dieser Instanz definierte, Server nicht erreichbar ist. Geben Sie für den sekundären Server folgende Angaben ein:
   - Name oder IP-Adresse
   - Port
   - Gemeinsamer geheimer Schlüssel

   Hinweis: Für diesen sekundären RADIUS-Server müssen Sie eine Instanz festlegen.
10. Klicken Sie auf **Save Changes**. Wenn Sie zum ersten Mal eine Serverinstanz erstellen, werden die Registerkarten **Settings** und **Users** angezeigt.
11. Konfigurieren Sie den primären und den sekundären RADIUS-Server für die Erkennung des IVE. Folgen Sie hierfür den folgenden Anweisungen.
12. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 273).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen“ auf Seite 263.

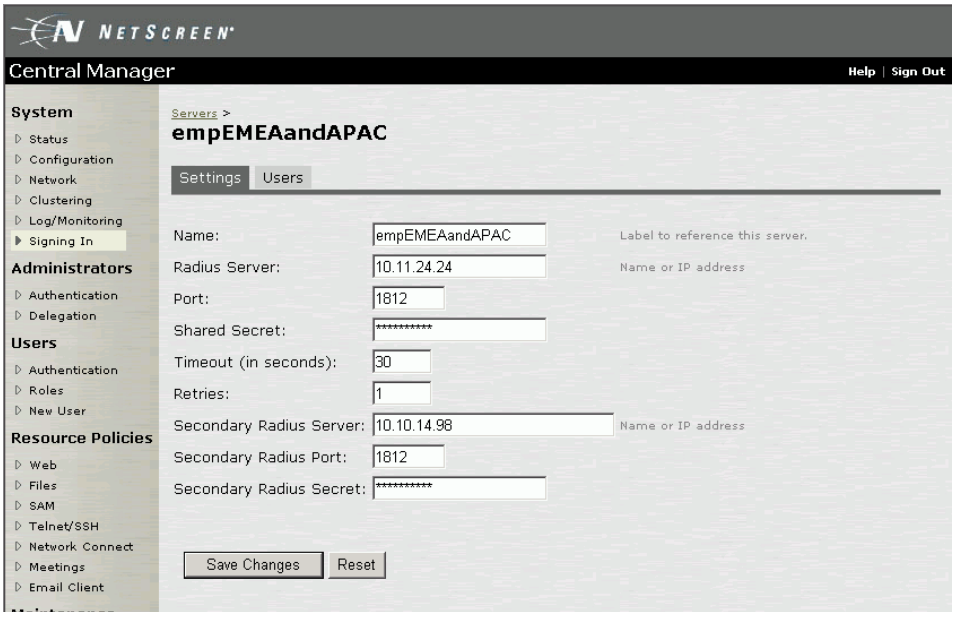


Abbildung 63: System > Signing In > Servers > Radius Server

☑ Konfigurieren des RADIUS-Servers für die Erkennung des IVE

Sie müssen den RADIUS-Server durch folgende Angaben für die Erkennung des IVE appliance-Servers konfigurieren:

- Hostname der IVE appliance.
- Netzwerk-IP-Adresse der IVE appliance.
- Clienttyp der IVE appliance (sofern vorhanden). Wenn diese Option verfügbar ist, wählen Sie „Single Transaction Server" oder die entsprechende Option.
- Verschlüsselungstyp für die Authentifizierung der Clientkommunikation. Die ausgewählte Option muss mit dem Clienttyp übereinstimmen.
- Gemeinsamer geheimer Schlüssel, der an der Web console auf der Seite **System > Signing In > Servers > Radius Server** für den RADIUS-Server eingegeben wurde.

Konfigurieren einer Netegrity SiteMinder-Instanz

Die folgenden Themen werden behandelt:

Netegrity SiteMinder – Übersicht....247
Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver ..252
Konfiguration des IVE, sodass Benutzer mit niedriger Sicherheitsebene sich neu authentifizieren müssen 253
Festlegen einer Netegrity SiteMinder-Instanz 255
Einrichten von erweiterten SiteMinder-Konfigurationsoptionen....260

Netegrity SiteMinder – Übersicht

Bei der Benutzerauthentifizierung eines Benutzers mit einem Netegrity SiteMinder-Server überprüft das IVE auf der Anmeldeseite eingegebene Benutzername und das Kennwort über einen Netegrity SiteMinder-Server, bevor es ggf. Zugriff gewährt. Bei der Authentifizierung leitet das IVE die Anmeldeinformationen an den Netegrity SiteMinder-Server weiter, um Benutzern Authentifizierung per Einzelanmeldung über SiteMinder zu ermöglichen. Der SiteMinder-Server kann Standard-Netegrity-Authentifizierung, ACE SecurID-Tokens oder clientseitige Zertifikate zur Authentifizierung der Anmeldeinformationen verwenden, die vom IVE weitergeleitet wurden, wie unter „Authentifizierung mit mehreren Authentifizierungsschemas“ auf Seite 248erläutert.

Wenn ein Benutzer über einen SiteMinder-Server mit einer bestimmten Sicherheitsebene authentifiziert wird, erhält der Benutzer nahtlosen Zugriff auf SiteMinder-Webressourcen, die Sicherheitsebene entsprechen oder eine niedrigere Sicherheitsebene aufweisen. Wenn ein Benutzer versucht, auf eine Webressource einer höheren Sicherheitsebene zuzugreifen, kann auch eine erneute Authentifizierung über das IVE erfolgen, wie unter „Konfiguration des IVE, sodass Benutzer mit niedriger Sicherheitsebene sich neu authentifizieren müssen“ auf Seite 253 erläutert.

Die IVE appliance ermöglicht die Einzelanmeldung bei Netegrity-geschützten Ressourcen, indem es Netegrity SiteMinder Security-Token (auch als SMSESSION-Cookies bezeichnet) speichert. Die IVE appliance stellt eine Verbindung mit dem Web-Agent her, der in der Webkonsole angegeben wurde, und sendet die Anmeldinformationen an den Web-Agent weiter, sobald sich ein Benutzer bei der IVE applianceanmeldet. Wenn die Anmeldeinformationen authentifiziert werden können, übergibt der Web-Agent ein SMSESSION-Cookie an die IVE appliance, die es überprüft und anschließend speichert. Beim Versuch des Benutzers, auf eine Webressource auf einem Standard-Web-Agent zuzugreifen, übergibt die IVE appliance das Cookie zur Authentifizierung an den Web-Agent.

SMSESSION-Cookies speichern verschiedene Benutzerinformationen, darunter Benutzername, Kennwort und autorisierte Sicherheitsebenen. SMSESSION-Cookies können auf zwei Wegen erstellt und an den Browser des Benutzers übermittelt werden: Anhand des benutzerdefinierten IVE-Agents, der mithilfe des Netegrity SDK erstellt wurde, oder anhand anderer Standard-Web-Agents, wie unter „Automatische Anmeldung beim IVE mithilfe von SiteMinder-Authentifizierung“ auf Seite 249 erläutert.

Sie können das IVE bei Bedarf auch so konfigurieren, dass es Anmeldeinformationen von SiteMinder akzeptiert und somit die Möglichkeit zur Einzelanmeldung von SiteMinder für das IVE ermöglichen, wie unter „Automatische Anmeldung beim IVE über SiteMinder“ auf Seite 250. erläutert.

Wichtig: Zur Zeit der Drucklegung dieses Dokuments bietet NetScreen Unterstützung für Netegrity Siteminder-Server, Version 5.5 mit Standard-Agent-Versionen 5QMR5 und 4QMR6, und ist mit Netegrity Siteminder-Server, Version 4.61, kompatibel.

Authentifizierung mit mehreren Authentifizierungsschemas

Ein ***Authentifizierungsschema*** bietet in SiteMinder eine Möglichkeit, Anmeldinformationen zu sammeln und die Identität eines Benutzers zu ermitteln. Sie können verschiedene Authentifizierungsschemas erstellen und ihnen jeweils verschiedene Sicherheitsebenen zuordnen. Sie können z.B. zwei Schemas erstellen: eins, das Benutzer nur auf Grundlage ihrer clientseitigen Zertifikate authentifiziert und sie mit einer niedrigen Sicherheitsebene versieht, und ein zweites, das ACE SecurID-Tokenauthentifizierung verwendet und eine höhere Sicherheitsebene bereitstellt. Das IVE funktioniert mit folgenden Arten von SiteMinder-Authentifizierungsschemas:

- **Einfache Authentifizierung über Benutzername und Kennwort**

  Benutzername und Kennwort werden an den SiteMinder-Richtlinienserver weitergeleitet. Der Richtlinienserver kann diese dann selbst authentifizieren oder sie zur Authentifizierung an einen anderen Server weiterleiten (Seite 250).

- **ACE SecurID-Token-Authentifizierung**

  Der SiteMinder-Richtlinienserver authentifiziert Benutzer auf Grundlage von Benutzername und Kennwort, die von einem ACE SecurID-Token generiert werden.

- **Authentifizierung über clientseitige Zertifikate**

  Der SiteMinder-Richtlinienserver authentifiziert Benutzer auf Grundlage ihrer Anmeldeinformationen des clientseitigen Zertifikats[1]. Wenn Sie diese Authentifizierungsmethode auswählen, zeigt das IVE Benutzern weiterhin die Standardanmeldeseite mit der Eingabeaufforderung für Benutzernamen und Kennwort[2] an. Benutzer können diese Felder jedoch einfach leer lassen und auf **Submit** klicken kann, sofern weder das IVE noch der SiteMinder-Server die Eingabe von Benutzername und Kennwort erfordern.

  Wichtig: Wenn Benutzer anhand dieser Methode authentifiziert werden sollen, müssen Sie die Zertifikate der Zertifizierungsstelle ins IVE importieren. Verwenden Sie hierfür die Registerkarte **System > Certificates > CA Certificates** (Seite 153).

Wichtig: Um das IVE so zu konfigurieren, dass es mit verschiedenen Authentifizierungsschemas arbeitet, ordnen Sie jedem SiteMinder-Authentifizierungsschema einen IVE-Anmelde-URL zu. Während der Produktion wird folgendermaßen verfahren:

1. Der Benutzer wählt einen der Bereiche aus, indem er sich unter einem dem Bereich zugeordneten URL anmeldet oder indem er einen Bereich aus einer Dropdownliste auf der IVE-Anmeldeseite auswählt.
2. Das IVE sendet die geschützte Ressource, die dem ausgewählten Bereich zugeordnet ist, an SiteMinder.
3. SiteMinder bestimmt anhand der Ressource die Art des Authentifizierungsschemas, die verwendet werden soll, und die Sicherheitsebene des Benutzers.
4. Das IVE sammelt die für das Authentifizierungsschema erforderlichen Anmeldinformationen und leitet sie zur Authentifizierung an SiteMinder weiter.

Automatische Anmeldung beim IVE mithilfe von SiteMinder-Authentifizierung

Um Einzelanmeldung vom IVE bei SiteMinder zu ermöglichen, muss ein Web-Agent SMSESSION-Cookies erstellen und an den Browser des Benutzers senden. SMSESSION-Cookies können auf zwei Wegen erstellt und an den Browser des Benutzers übermittelt werden. Entweder durch

1. Die SiteMinder-Authentifizierung über clientseitige Zertifikate läuft getrennt von der IVE-Authentifizierung über clientseitige Zertifikate.
2. Wenn Benutzern nicht die IVE-Standardanmeldeseite angezeigt werden soll, können Sie diese mit den Funktionen zum Anpassen der Benutzeroberfläche ändern, die Ihnen auf der NetScreen-Supportseite zur Verfügung stehen.

SiteMinder oder durch den benutzerdefinierten IVE Web-Agent mithilfe des folgenden Verfahrens:

- **Authentifizierung anhand des benutzerdefinierten Agent** (Seite 257)

  Die IVE appliance verwendet einen benutzerdefinierten Web-Agent, der mithilfe des Netegrity Software Development Kit (SDK) erstellt wurde. Wenn sich ein Benutzer bei einer IVE applianceanmeldet, leitet der benutzerdefinierte Web-Agent die Benutzeranmeldeinformationen an den SiteMinder-Richtlinienserver weiter. Wenn die Anmeldeinformationen authentifiziert werden, erstellt der benutzerdefinierte Web-Agent ein SMSESSION-Cookie und speichert es in der IVE appliance. Beim Versuch des Benutzers, auf eine Webressource auf einem Standard-Web-Agent zuzugreifen, übergibt die IVE appliance das Cookie zur Authentifizierung an den Web-Agent.

  Wichtig: Wenn Sie diese Option auswählen, müssen Sie Ihren Web-Agent mit dem entsprechenden Siteminder Agent Quarterly Maintenance Release (QMR) aktualisieren, damit dieser unser Cookie erkennen kann.

  - Web-Agents für SiteMinder, Version 4 – Verwenden Sie den QMR-Patch „V4QMR4-010.zip", der über die Netegrity-Website verfügbar ist. (Möglicherweise müssen Sie auch vorausgesetzte Hotfixes installieren, wie etwa „V4QMR4-Windows.zip".)
  - Web-Agents für SiteMinder, Version 5 – Verwenden Sie das QMR5-Hotfix (bei Netegrity seit dem 30. September 2002 erhältlich).

  Beachten Sie auch, dass Sie das Attribut „Accept Third Party Cookie" (`AcceptTPCookie`) in der Web-Agent-Konfigurationsdatei (`webagent.conf`) auf `yes` oder in der Windows-Registrierung auf 1 für den IIS-Webserver setzen müssen. Der Speicherort dieses Attributs hängt von der verwendeten SiteMinder-Version und dem Webserver ab. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.

- **Authentifizierung mithilfe der Option „HTML Form Post"** (Seite 257)

  Die IVE appliance generiert kein SMSESSION-Cookie, sondern ruft das Cookie von einem anderen Web-Agent ab. Beachten Sie Folgendes, wenn Sie die Option **Authenticate using HTML form post** aktivieren:

  - Dies wird nicht in Kombination mit der Authentifizierung über clientseitige Zertifikate unterstützt.
  - SecurID New Pin- und Next Token-Modi werden nicht unterstützt.

Automatische Anmeldung beim IVE über SiteMinder

Um die Einzelanmeldung von einem anderen Web-Agent am IVEzu ermöglichen, muss das IVE ein vorhandenes SMSESSION-Cookie prüfen, das von einem Standard-Web-Agent von SiteMinder, Version 4.x oder 5.x erstellt

wurde. Bei der Auswahl der Option **Automatic Sign in** (Seite 256) kann der Benutzer, wenn er sich bereits an einem anderen Netegrity-fähigen Server in der gleichen Domäne wie die IVE appliance angemeldet hat, ohne Aufforderung zur einer erneuten Anmeldung auf die IVE appliance zugreifen. Die IVE appliance überprüft lediglich anhand des Richtlinienservers das vom Browser des Benutzers gesendete SMSESSION-Cookie. Alle Benutzer, die sich auf diese Weise beim IVE anmelden, werden dem Bereich zugeordnet, der auf der Registerkarte **System > Signing In > Servers > [SiteMinder-Server]** der IVE-Webkonsole angegeben ist, und ihnen wird eine Rolle zugewiesen, die auf den Einstellungen auf der Registerkarte **Users > Authentication > [Bereich] > Role Mapping** basiert.

Wenn Sie die Option **Automatic Sign in** aktivieren, müssen Sie Folgendes beachten:

- Wenn sich ein Benutzer automatisch an einem URL anmeldet, der mehreren Authentifizierungsbereichen zugeordnet ist, meldet das IVE den Benutzer an demjenigen Bereich an, der auf der Registerkarte **System > Signing In > Servers > [SiteMinder-Server]** in der IVE-Webkonsoleangegeben ist, (***nicht*** an dem URL, der auf der Registerkarte **System >Signing In > Sign-in Policies** angegeben ist).
- Wenn die Sicherheitsebene, die dem SMSESSION-Cookie eines Benutzers zugeordnet ist, von der Sicherheitsebene des IVE-Bereichs abweicht, verwendet das IVE die Sicherheitsebene, die dem Cookie zugeordnet ist.

Abrufen des korrekten Benutzernamens für Einzelanmeldung

Wenn verschiedene Authentifizierungsschemas und Anmeldepunkte verfügbar sind, kann das IVE für ein und denselben Benutzer durchaus unterschiedliche Benutzernamen empfangen. Für den Fall, dass das IVE denselben Benutzernamen für verschiedene Server verwendet, wird vorzugsweise der von SiteMinder bereitgestellte Name verwendet. Wenn ein Benutzer Folgendes vornimmt:

- **Anmeldung über die Standard-IVE-Anmeldeseite** – Das IVE gibt dem Benutzernamen den Vorzug, den SiteMinder im `OnAuthAccept`-Header zurückgibt. Wenn SiteMinder keinen Benutzernamen bereitstellt, verwendet das IVE den Benutzernamen, den der Benutzer bei der Anmeldung eingegeben hat. Andernfalls, wenn also weder SiteMinder noch der Benutzer einen Benutzernamen angeben, verwendet das IVE den Benutzer-DN, den der Richtlinienserver zurückgibt. (Dies kommt nur dann vor, wenn Sie festgelegt haben, dass Benutzer auf dem SiteMinder-Server anhand eines Zertifikats von einer Zertifizierungsstelle authentifiziert werden.)

- **Anmeldung beim IVE anhand der SiteMinder-Anmeldeinformationen** – Das IVE gibt demjenigen Benutzernamen den Vorzug, den SiteMinder im `OnAuthAccept`-Header zurückgibt. Wenn SiteMinder keinen Benutzernamen bereitstellt, verwendet das IVE den Benutzernamen im SMSESSION-Cookie. Ansonsten verwendet es die den Benutzer-DN im SMSESSION-Cookie.

Um den korrekten Benutzernamen weiterzuleiten, konfigurieren Sie folgende Optionen auf dem Richtlinienserver für den IVE-Web-Agent:

1. Navigieren Sie zum Bereich mit der Ressource */ive-authentication*.
2. Erstellen Sie eine neue Regel, in der Folgendes gilt:
   - Action=Authentifizierungsereignis
   - OnAuthAccept ist aktiviert
3. Erstellen Sie eine neue Antwort, in der Folgendes gilt:
   - Attribute Name = WebAgent-HTTP-Header-Variable
   - Variable Name = IVEUSERNAME

Zusatzinformationen

- Netegrity speichert die IP-Adresse nicht im SMSESSION-Cookie und kann sie daher nicht an die IVE-Appliance übergeben.
- SiteMinder sendet das SMSESSION-Cookie als dauerhaftes Cookie an das IVE. Um ein Höchstmaß an Sicherheit zu gewährleisten, setzt das IVE das dauerhafte Cookie nach Abschluss der Authentifizierung zu einem Sitzungscookie zurück.
- Das IVE unterstützt weder W-SAM noch Network Connect oder Authentifizierungs-Vorabprüfungen durch die Hostprüfung bzw. Cachebereinigung mit der Funktion **Automatic Sign in**.

☑ Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver

Sie können einen SiteMinder-Server erst als IVE-Authentifizierungsserver hinzufügen, wenn Sie das IVE auf dem SiteMinder-Richtlinienserver als Agent konfiguriert haben. Das folgende Verfahren enthält die grundlegenden Schritte zur Konfiguration eines SiteMinder-Richtlinienservers. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SiteMinder-Server.

So konfigurieren Sie das IVE als Web-Agent auf einem SiteMinder-Richtlinienserver:

1. Melden Sie sich auf der Benutzeroberfläche des Richtlinienservers an.
2. Erstellen Sie einen Agent für das IVE. Wenn Sie SiteMinder, Version 5, verwenden, erstellen Sie ein Hostkonfigurationsobjekt, oder duplizieren Sie ein vorhandenes Hostkonfigurationsobjekt, und ändern Sie die Parameterwerte.
3. Konfigurieren Sie eine neue Richtliniendomäne, oder verwenden Sie eine vorhandene Richtliniendomäne.
4. Erstellen Sie unterhalb der Richtliniendomäne einen SiteMinder-Bereich. Legen Sie den Ressourcenfilter auf „/" fest, und legen Sie dann eine GET-Regel fest, um alle Ressourcen mit „*" zu schützen. Verwenden Sie „/ive-authentication", um die IVE-Standardeinstellung zuzuordnen. Wenn Sie die Einstellungen für den SiteMinder-Authentifizierungsserver später in der Webkonsolekonfigurieren, müssen Sie die entsprechenden Einstellungen für das Feld **Protected Resource** verwenden.
5. Erstellen Sie unterhalb der Richtliniendomäne eine Richtlinie, die die Regeln zu vorhandenen Benutzerverzeichnissen zuordnet.

☑ Konfiguration des IVE, sodass Benutzer mit niedriger Sicherheitsebene sich neu authentifizieren müssen

Während der Konfiguration des IVE müssen Sie eine geschützte Ressource (URL) angeben, um die Sicherheitsebene zu steuern, die für die SiteMinder-Sitzung des Benutzers zugelassen ist. Das IVE extrahiert den relevanten Abschnitt des URL (alle auf den Domänennamen folgenden Angaben) und übergibt ihn zur Authentifizierung an SiteMinder. SiteMinder gewährt dem Benutzer dann eine Sicherheitsebene, die dem URL entspricht.

Wenn ein Benutzer versucht, auf eine Webressource zuzugreifen, die eine höhere Sicherheitsebene erfordert als seine Zugriffsrechte erlauben, kann die erneute Authentifizierung über das IVE erfolgen, indem es ihn auf eine Seite mit folgenden Optionen weiterleitet:

- **Continue** – Wenn ein Benutzer diese Option auswählt, meldet das IVE ihn bei der aktuellen Sitzung ab und fordert die Eingabe der Anmeldinformationen, die für die Ressource der höheren Sicherheitsebene erforderlich sind. Wenn die Anmeldeinformationen authentifiziert werden können, leitet es ihn auf die Seite weiter, auf die er ursprünglich zugreifen wollte.
- **Cancel** – Wenn der Benutzer diese Option auswählt, wird er zur vorherigen Seite umgeleitet.

Wenn Sie sich hingegeben festlegen, dass keine erneute Authentifizierung über das IVE erfolgen soll, hängt der erneute Authentifizierungsprozess davon ab, ob der Richtlinienserver einen Authentifizierungsschema-URL an den Benutzer zurückgibt. Wenn auf dem Richtlinienserver Folgendes vorgeht:

- **Keine Rückgabe eines Authentifizierungsschema-URL** – Das IVE sendet dann Meldung über die fehlgeschlagene Validierung an den Benutzer zurück und führt die erneute Authentifizierung über die Standardseite `welcome.cgi` durch. Der Benutzer wird aufgefordert, sich erneut anzumelden, wobei ihm allerdings die ursprüngliche Sicherheitsebene zugeordnet wird und er möglicherweise immer noch keinen Zugriff auf die gewünschte Seite hat.
- **Rückgabe eines Authentifizierungsschema-URL** – Das IVE leitet den Benutzer an einen Standard-Web-Agent um, über den die erneute Authentifizierung erfolgen soll.

So erfolgt die erneute Authentifizierung über das IVE:

1. Legen Sie auf der Seite **System > Signing In > Sign-in Policies** der Webkonsole einen Anmelde-URL für die SiteMinder-Serverinstanz fest (Seite 203).
2. Definieren Sie ein Authentifizierungsschema auf dem SiteMinder-Richtlinienserver anhand der folgenden Parameter:
   - Geben Sie die gewünschte Sicherheitsebene eine (z.B. 30).
   - Aktivieren Sie das Kontrollkästchen **Password Policies Enabled**.
   - Geben Sie unter **Server Name** den Hostnamen des IVE ein (z.B. vertrieb.firmenname.net).
   - Aktivieren Sie das Kontrollkästchen **Use SSL Connection**.
   - Geben Sie unter **Target** den im ersten Schritt definierten Anmelde-URL des IVE und den Parameter „ive=1" ein (z.B. /highproturl?ive=1).

     Hinweis: Wenn Sie Änderungen speichern, wird `ive=1` nicht mehr für das Ziel angezeigt. Das ist richtig. Der Richtlinienserver fügt `ive=1` in den vollständigen Authentifizierungsschema-URL ein, den er an das IVE sendet, wie auf der Registerkarte **Advanced** im Feld **Parameter** ersichtlich ist.

   - Deaktivieren Sie das Kontrollkästchen **Allow Form Auth Scheme to Save Credentials**.
   - Lassen Sie die Liste **Additional Attribute** leer.

☑ Festlegen einer Netegrity SiteMinder-Instanz

So legen Sie eine Netegrity SiteMinder-Serverinstanz fest:

1. Konfigurieren Sie das IVE als Agent auf dem SiteMinder-Richtlinienserver. Folgen Sie hierfür den Anweisungen unter „Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver“ auf Seite 252.
2. Wählen Sie in der Webkonsole **System > Signing In > Servers** aus.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Um eine neue Serverinstanz auf dem IVE zu erstellen, wählen Sie aus der Liste **New** den Eintrag **SiteMinder Server** aus, und klicken Sie dann auf **New Server**.
   - Klicken Sie zum Aktualisieren einer vorhandenen Serverinstanz auf die entsprechende Verknüpfung in der Liste **Authentication/Authorization Servers**.
4. Geben Sie im Feld **Name** einen Namen ein, der die Serverinstanz bezeichnet.
5. Geben Sie im Feld **Policy Server** den Namen oder die IP-Adresse des SiteMinder-Richtlinienservers ein, den Sie zur Benutzerauthentifizierung verwenden möchten.
6. Geben Sie im Feld **Backup Server(s)** eine durch Kommas getrennte Liste von Richtlinienservern ein (optional). Wählen Sie dann einen **Failover Mode** aus.
   - Wählen Sie **Yes** aus, damit die IVE appliance den Hauptrichtlinienserver verwendet, sofern dieser betriebsbereit ist.
   - Wählen Sie **No** aus, damit die IVE appliance einen Lastenausgleich zwischen allen Richtlinienservern vornimmt.
7. Legen Sie das freigegebene **Secret** und den **Agent Name** fest, wie unter „Konfigurieren des IVE als Web-Agent auf einem SiteMinder-Richtlinienserver“ auf Seite 252 dargestellt.
8. Legen Sie im Feld **On logout, redirect to** einen URL fest, auf den Benutzer umgeleitet werden, wenn sie sich vom IVE abmelden (optional). Wenn Sie dieses Feld leer lassen, wird Benutzern die Standard-IVE-Anmeldeseite angezeigt (login.cgi).

Wichtig: Das Feld **On logout, redirect to** befindet sich aus Gründen der Abwärtskompatibilität in Produktversion 4.0, wird in zukünftigen Versionen jedoch nicht mehr enthalten sein. Wenn Sie Benutzer nach der Abmeldung auf eine andere Anmeldeseite umleiten möchten, empfiehlt es sich dringend, stattdessen die Funktion **Custom Pages** zu verwenden (Seite 209).

---

9. Geben Sie im Feld **Protected Resource** eine geschützte Ressource ein (Seite 253). Das IVE verwendet diesen URL, um die Sicherheitsebene des Benutzers für die jeweilige Sitzung festzulegen. Wenn die Benutzer sich an dem URL „*" (Standard-IVE-Anmeldeseite) anmelden, geben Sie `/ive-authentication` ein.
10. Beachten Sie bei **Resource Action**, dass die Ressourcenaktion bei einem neuen SiteMinder-Server GET lautet (schreibgeschützt). Wenn die SiteMinder-Instanz von einer 3.x-Instanz aktualisiert wird, ist die Ressourcenaktion (GET, POST, PUT, usw.) dieselbe wie die bereits zuvor verwendete.

   Hinweis: Um eine vorhandene Ressourcenaktion auf GET zu ändern, müssen Sie sie löschen und eine neue SiteMinder-Serverinstanz erstellen.

11. Geben Sie im Feld **Cookie Domain** die Cookiedomäne des IVE ein. Beachten Sie dabei Folgendes:
    - Mehrere Domänen müssen durch Kommas getrennt werden (z.B. „vertrieb.eigeneorg.com, marketing.eigeneorg.com").
    - Bei Domänennamen wird die Groß- und Kleinschreibung berücksichtigt.
    - Es dürfen keine Platzhalterzeichen verwendet werden.
12. Geben Sie im Feld **Cookie Provider Domain** die Internetdomäne(n) an, an die die IVE appliance die Inhalte der SMSESSION-Cookies sendet. Wenn Sie für einen Cookieanbieter die Einzelanmeldung über mehrere Cookiedomänen aktiviert haben, geben Sie den Namen des Cookieanbieters ein. Andernfalls geben Sie die Domäne(n) der Web-Agents ein, für die Einzelanmeldung erwünscht ist.
13. Wählen Sie im Abschnitt **Protocol** die Option **HTTPS**, um Cookies sicher zu senden, sofern andere Web-Agents für den Empfang sicherer Cookies eingerichtet sind, oder wählen Sie **HTTP** aus, um Cookies ungesichert zu senden.
14. Aktivieren Sie das Kontrollkästchen **Automatic Sign-In**, wenn Benutzer, die über ein gültiges SMSESSION-Cookie verfügen, automatisch beim IVE angemeldet werden sollen. Wählen Sie dann den Authentifizierungsbereich aus, dem die Benutzer zugeordnet werden. Weitere Informationen und Einschränkungen zu diesen Optionen finden Sie unter „Automatische Anmeldung beim IVE über SiteMinder" auf Seite 250.

15. Wählen Sie eine der folgenden Cookie-Authentifizierungsmethoden aus:

- **Authenticate using custom agent** – Wählen Sie diese Option aus, wenn die Authentifizierung über den benutzerdefinierten Web-Agent des IVE erfolgen soll.
- **Authenticate using HTML form post** – Wählen Sie diese Option aus, wenn die Authentifizierung über einen anderen Web-Agent erfolgen soll. Geben Sie dann die Einstellungen für die Formularbereitstellung an:

Einstellung	Beschreibung
Target	URL auf dem externen, Netegrity-fähigen Webserver.
Protocol	Protokoll für die Kommunikation zwischen dem IVE und dem angegebenen Web-Agent. Verwenden Sie HTTP für die ungesicherte Kommunikation oder HTTPS für die sichere Kommunikation.
Webagent	Name des Web-Agents, von dem das IVE SMSESSION-Cookies abrufen soll. In diesem Feld kann keine IP-Adresse eingegeben werden. Wenn die IP-Adresse als Web-Agent angegeben wird, können manche Browser keine Cookies akzeptieren.
Port	Port 80 für HTTP oder Port 443 für HTTPS.
Path	Pfad der Web-Agent-Anmeldeseite.
Parameters	Post-Parameter, die bei der Anmeldung eines Benutzers gesendet werden. Standardmäßig verwendet das IVE die Variablen `_ _USER_ _`, `_ _PASS_ _` und `_ _TARGET_ _`. Diese Variablen werden durch den vom Benutzer auf der Anmeldeseite des Web-Agents eingegebenen Benutzernamen und das Kennwort sowie durch den im Feld **Target** angegebenen Wert ersetzt.

Weitere Informationen und Einschränkungen zu diesen Optionen finden Sie unter „Automatische Anmeldung beim IVE mithilfe von SiteMinder-Authentifizierung“ auf Seite 249.

16. Geben Sie im Feld **If authentication fails, redirect to** einen alternativen URL ein, zu dem die Benutzer umgeleitet werden, wenn das IVE sie nicht authentifizieren kann und vom SiteMinder-Richtlinienserver keine Umleitungsantwort eingeht. Wenn Sie dieses Feld leer lassen, werden die Benutzer aufgefordert, sich erneut beim IVE anzumelden.

Hinweis: Wenn Sie die Option für die Anpassung der Oberfläche verwenden (Seite 209), beachten Sie, dass das IVE noch in zwei weiteren Fällen auf die Seite `welcome.cgi` umleitet. Sie müssen beide Sonderfälle in Ihrer benutzerdefinierten Seite berücksichtigen:
Ablauf der Sitzungs- oder Leerlaufhöchstdauer: `/dana-na/auth/welcome.cgi?p=timed-out`.
Fehlgeschlagene Cookievalidierung: `/dana-na/auth/welcome.cgi?p=failed`

---

17. Aktivieren Sie das Kontrollkästchen **Authorize requests against SiteMinder policy server** , wenn die Regeln des SiteMinder-Richtlinienservers für die Autorisierung der Benutzeranforderungen von Webressourcen verwendet werden sollen. Wenn Sie diese Option auswählen, müssen Sie in SiteMinder die entsprechenden Regeln erstellen, die mit dem Servernamen, gefolgt von einem Schrägstrich beginnen, z.B.: „www.yahoo.com/", „www.yahoo.com/*" und „www.yahoo.com/r/f1".
18. Geben Sie im Feld **Resource for insufficient protection level** eine Ressource des Web-Agents ein, an die Benutzer vom IVE umgeleitet werden, wenn sie nicht über die erforderlichen Berechtigungen verfügen. Wenn der Benutzer auf eine Ressource zugreift, die eine höhere Sicherheitsebene als sein SMSESSION-Cookie hat, öffnet sich eine gesicherte Anmeldeseite. Nach der erneuten Authentifizierung erhält er ein SMSESSION-Cookie mit einer höheren Sicherheitsebene und wird auf eine Webseite umgeleitet. Die Art der Webseite, die das IVE anzeigt, hängt von der Konfiguration ab. Gehen Sie bei der erneuten Authentifizierung folgendermaßen vor:
    - **Standard-Web-Agent 4.x oder 5.x mit „FCCCompatMode = yes"**

      Geben Sie im Feld **Resource for insufficient protection level** eine Webseite auf diesem Standard-Web-Agent ein. Sie müssen dabei nicht den gesamten URL der Ressource (z.B. https://connect2.netscreen.com/,DanaInfo=www.stdwebagent.com+index.html), sondern nur die Ressource eingeben (index.html).

      In diesem Fall kann das IVE nach der erneuten Authentifizierung nur auf eine Webseite auf dem Standard-Web-Agent umleiten. Es kann nicht auf die Ressource umleiten, auf die der Benutzer ursprünglich zugreifen wollte.

- **Standard-Web-Agent 5.x (V5QMR3 oder höher) mit „FCCCompatMode = no"**

  Lassen Sie das Feld **Resource for insufficient protection level** leer, um auf die Ressource umzuleiten, auf die der Benutzer ursprünglich zugreifen wollte. Sie können auch eine statische Ressource eingeben.

- **IVE**

  Konfigurieren Sie den Richtlinienserver nach den Anweisungen unter „Konfiguration des IVE, sodass Benutzer mit niedriger Sicherheitsebene sich neu authentifizieren müssen" auf Seite 253.

19. Geben Sie im Feld **Ignore authorization for files with extensions** Dateierweiterungen von Dateitypen ein, für die keine Autorisierung erforderlich ist. Sie müssen die Erweiterung jedes einzelnen Dateityps eingeben, der ignoriert werden soll, und diese durch Kommas trennen. Geben Sie beispielsweise `.gif, .jpeg, .jpg, .bmp` ein, um verschiedene Bilddateitypen zu ignorieren. Es dürfen keine Platzhalterzeichen verwendet werden (wie etwa ***, *.*,** oder `.*`), um eine ganze Gruppe von Dateitypen zu ignorieren.
20. Klicken Sie auf **Save Changes**.
21. Richten Sie bei Bedarf erweiterte SiteMinder-Konfigurationsoptionen ein (Seite 260).
22. Geben Sie die Bereiche an, die der Server für die Authentifizierung und Autorisierung von Administratoren und Benutzern verwenden soll (Seite 275).

Hinweis: Informationen zum Überwachen und Löschen von Sitzungen von Benutzern, die zu diesem Zeitpunkt über den Server angemeldet sind, finden Sie unter „Anzeigen und Löschen von Benutzersitzungen" auf Seite 263.

☑ Einrichten von erweiterten SiteMinder-Konfigurationsoptionen

Beim Erstellen einer SiteMinder-Serverinstanz wird die Registerkarte **Advanced** angezeigt, auf der Sie erweiterte Einstellungen festlegen können. Die Registerkarte enthält folgende Felder:

- **Poll Interval** – Geben Sie das Intervall ein, nach dessen Ablauf das IVE den SiteMinder-Richtlinienserver auf neue Schlüssel abfragt.
- **Policy Server options** – Zur Leistungssteigerung können Sie ggf. die Einstellungen für die Verbindung und die Leerlaufhöchstdauer einstellen. Beachten Sie jedoch die empfohlenen Standardeinstellungen:
  - **Max. Connections** steuert die Höchstanzahl gleichzeitiger Verbindungen an, die das IVE mit dem Richtlinienserver herstellen kann. Der Standardwert lautet 20.
  - **Max. Requests/Connection** steuert die Höchstanzahl von Anforderungen, die die Richtlinienserververbindung verarbeitet, bevor das IVE die Verbindung trennt. Der Standardwert lautet 1000.
  - **Idle Timeout** steuert die Höchstanzahl von Minuten, für die sich eine Verbindung mit dem Richtlinienserver im Leerlauf befinden kann (d.h. keine Anforderungen verarbeitet), bevor das IVE die Verbindung trennt. Die Standardeinstellung „none" gibt an, dass es keine zeitliche Begrenzung gibt.
  - **Accounting Port**: Der Standardwert lautet 44441.
  - **Authentication Port**: Der Standardwert lautet 44442.
  - **Authentication Port**: Der Standardwert lautet 44443.
- **Flush Cache** – Hiermit kann der Ressourcencache des IVE gelöscht werden, in dem Ressourcenautorisierungsdaten 10 Minuten lang zwischengespeichert werden.

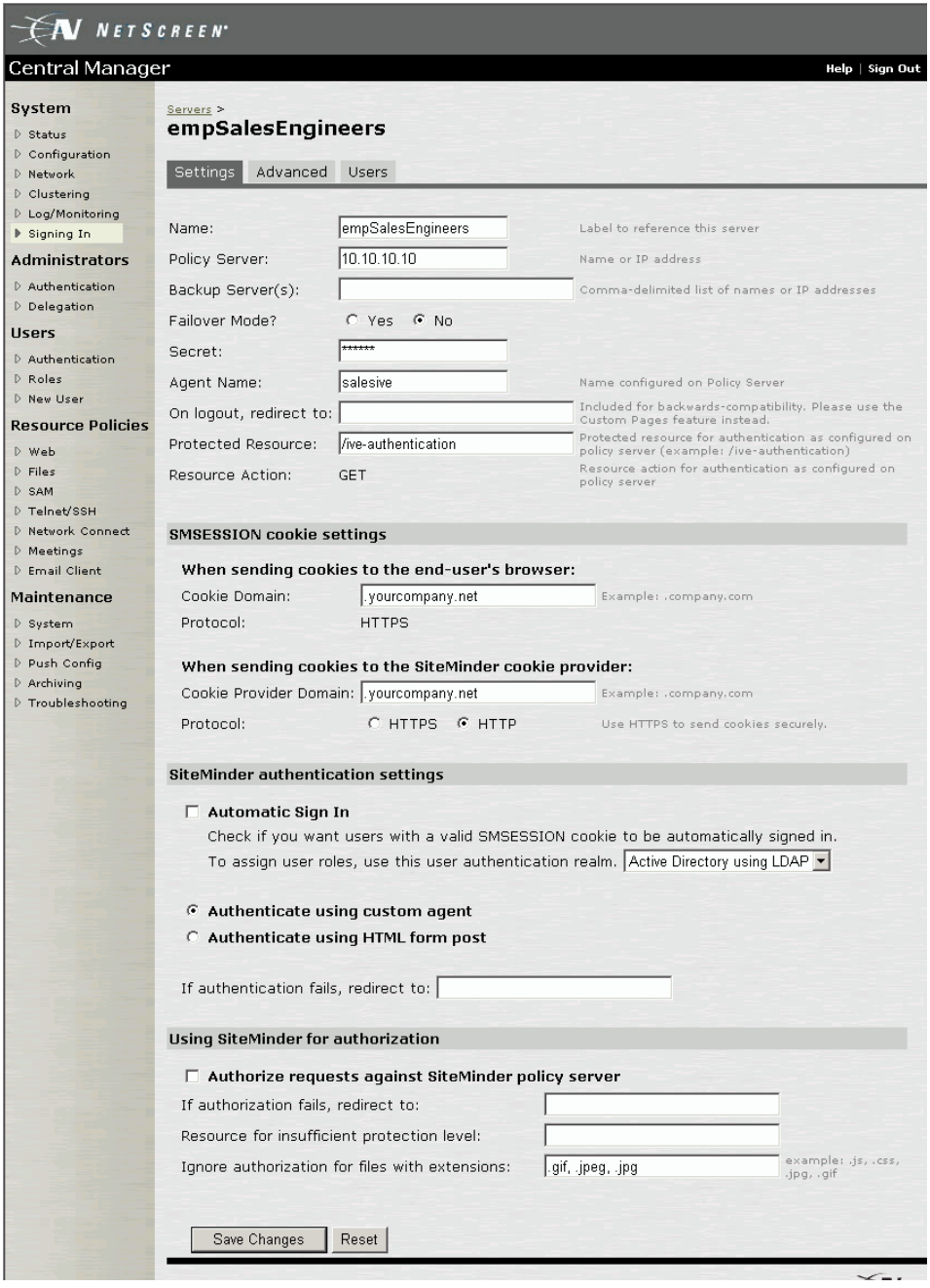


Abbildung 64: System > Signing In > Servers > SiteMinder Server

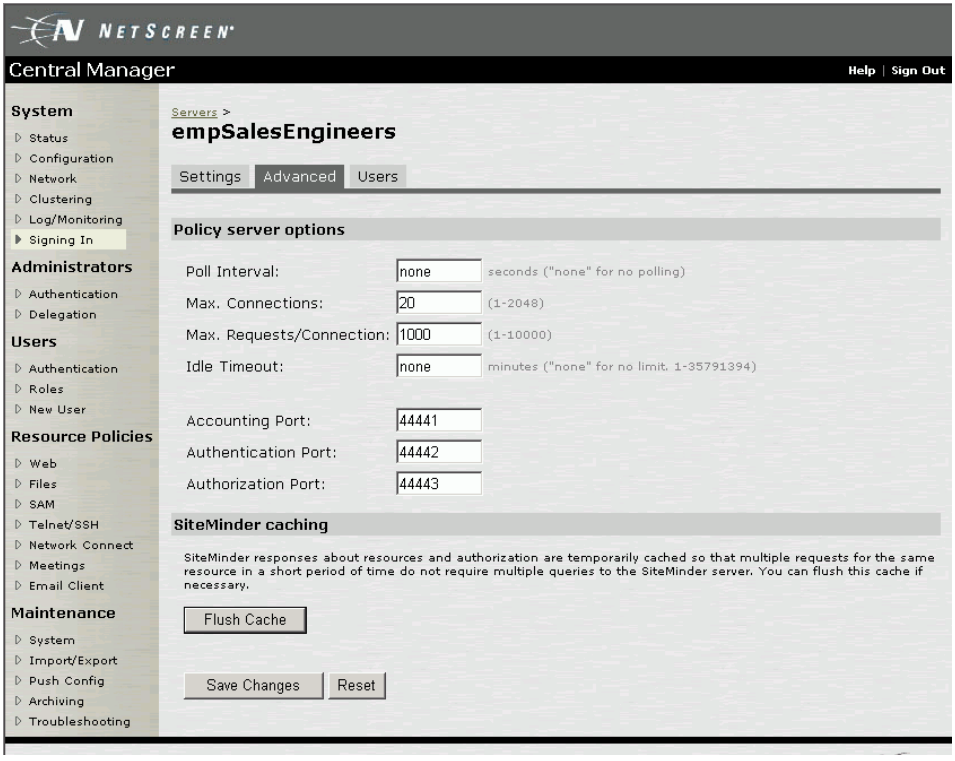


Abbildung 65: System > Signing In > Servers > SiteMinder Server > Advanced

Anzeigen und Löschen von Benutzersitzungen

☑ Anzeigen und Löschen aktiver IVE-Benutzersitzungen

Die Konfigurationsseite für die meisten IVE-Authentifizierungsserver enthält eine Registerkarte **Users**, auf der Sie aktive IVE-Benutzersitzungen anzeigen und löschen können. Auf den folgenden Typen von Authentifizierungsservern wird diese Registerkarte nicht angezeigt:

- **Anonymer Server** – Das IVE kann keine individuellen Sitzungsdaten für Benutzer anzeigen, die sich über einen anonymen Server anmelden, da bei der Benutzeranmeldung über einen anonymen Server keine Benutzernamen oder anderen Anmeldeinformationen erfasst werden.
- **Lokaler IVE-Server** – Das IVE zeigt für lokale IVE-Server statt einer Registerkarte **Users** eine Registerkarte **Local Users** an, auf der Sie Benutzerkonten (anstelle von Benutzersitzungen) hinzufügen und löschen können.

Bei sämtlichen anderen Typen von Authentifizierungsservern können Sie aktive Benutzersitzungen anzeigen und löschen. Folgen Sie hierfür den folgenden Anweisungen.

So zeigen Sie eine aktive Benutzersitzung an oder löschen sie:

1. Wählen Sie in der Web console **System > Signing In > Servers** aus.
2. Klicken Sie in der Liste **Authentication/Authorization Servers** auf die entsprechende Verknüpfung.
3. Klicken Sie auf die Registerkarte **Users**.
4. Führen Sie eine der folgenden Aufgaben durch:
   - Geben Sie im Feld **Show Users Named** einen Benutzernamen ein, und klicken Sie auf **Update**, um nach einem bestimmten Benutzer zu suchen.

     Sie können auch ein Sternchen (`*`) als Platzhalter verwenden, das für eine beliebige Anzahl von Zeichen steht (null, eins oder mehrere). Wenn Sie z.B. nach allen Benutzernamen suchen möchten, die die Buchstaben `jo` enthalten, geben Sie im Feld **Show users named** die Zeichenfolge `*jo*` ein. Bei der Suche wird die Groß- und Kleinschreibung berücksichtigt. Wenn Sie wieder die Gesamtliste der Gruppenkonten anzeigen möchten, geben Sie ein Sternchen (`*`) ein, oder löschen Sie den Feldinhalt, und klicken Sie dann auf **Update**.
   - Geben Sie im Feld **Show N users** eine Zahl ein, und klicken Sie auf **Update**, um die Anzahl von Benutzern anzugeben, die auf der Seite angezeigt werden.

- Aktivieren Sie das Kontrollkästchen neben den jeweiligen Benutzern, und klicken Sie anschließend auf **Delete**, um deren IVE-Sitzungen zu beenden.

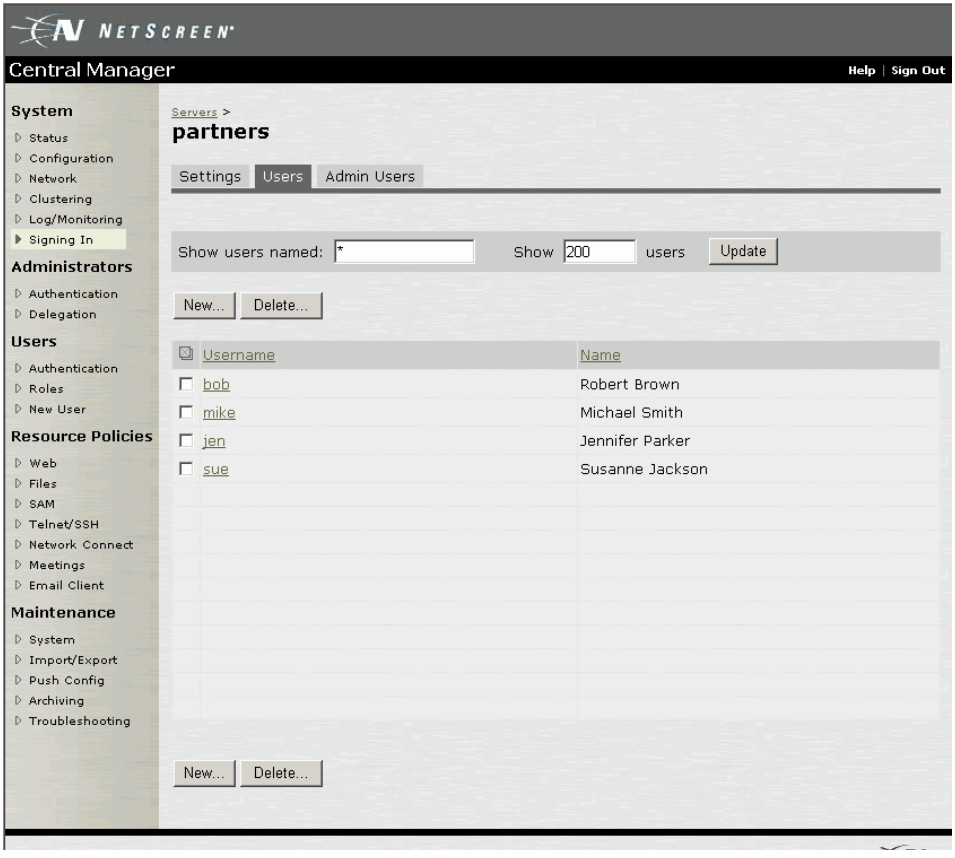


Abbildung 66: System > Signing In > Servers > [Ausgewählter Server] > Users

Konfigurieren der Seite „Delegation“

Auf der Seite **Administrators > Delegation** können Sie Administrationsberechtigungen (schreibgeschützt, lese- und schreibberechtigt, abzulehnen) für verschiedene Systemaufgaben wie Netzwerkbetrieb, Einrichtung von Clustern und Protokollierung sowie für die Funktionen zum Verwalten der auf dem System definierten Benutzerrollen festlegen. Weitere Informationen finden Sie unter „Delegierte Administration – Übersicht“ auf Seite 83.

Die Seite **Administrators > Delegation** enthält die folgenden Registerkarten:

Registerkarte „General“ 268
Registerkarte „System“ 268
Registerkarte „User Role Admin“ 271

Auf den Registerkarten der Seite **Administrators > Delegation** können Sie die folgenden Aufgaben durchführen:

Erstellen, Ändern und Löschen von Administratorrollen 265
Konfigurieren allgemeiner Einstellungen für eine Administratorrolle 268
Delegieren von Verwaltungsaufgaben an eine Administratorrolle 268
Delegieren von Benutzerrollenverwaltung an eine Administratorrolle 271

☑ Erstellen, Ändern und Löschen von Administratorrollen

Wenn Sie zu **Administrators > Delegation** navigieren, wird die Seite **Delegated Admin Roles** angezeigt. Auf dieser Seite können Sie Administratorrollen erstellen, ändern und löschen sowie Standardoptionen für Sitzungen und Benutzeroberfläche für delegierte Administratorrollen festlegen.

So erstellen Sie eine Administratorrolle:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie zum Erstellen einer neuen Administratorrolle mit den Standardeinstellungen auf **New Role**.
   - Aktivieren Sie das Kontrollkästchen neben einer vorhandenen Administratorrolle, und klicken Sie auf **Duplicate**, um die Rolle und benutzerdefinierten Berechtigungen zu kopieren.
3. Geben Sie unter **Name** einen Namen (erforderlich) und unter **Description** eine Beschreibung (optional) für die neue Rolle ein, und klicken Sie auf **Save Changes**.

4. Ändern Sie die Rolleneinstellungen nach den Anweisungen in:
   - „Registerkarte „General““ auf Seite 268
   - „Registerkarte „System““ auf Seite 268
   - „Registerkarte „User Role Admin““ auf Seite 271

So ändern Sie eine vorhandene Administratorrolle:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Klicken Sie auf den Namen der zu ändernden Administratorrolle.
3. Ändern Sie die Rolleneinstellungen nach den Anweisungen in:
   - „Registerkarte „General““ auf Seite 268
   - „Registerkarte „System““ auf Seite 268
   - „Registerkarte „User Role Admin““ auf Seite 271

So löschen Sie eine vorhandene Administratorrolle:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Aktivieren Sie das Kontrollkästchen neben der zu löschenden Administratorrolle, und klicken Sie auf **Delete**.
3. Klicken Sie auf **Delete**, um das Entfernen der ausgewählten Rolle zu bestätigen.

So legen Sie die Standardoptionen für delegierte Administratorrollen fest:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Klicken Sie auf **Default Options**.
3. Ändern Sie die Einstellungen auf den Registerkarten **Session Options** und **UI Options**. Diese stellen ab jetzt die neuen Standardwerte für alle neuen delegierten Administratorrollen dar.

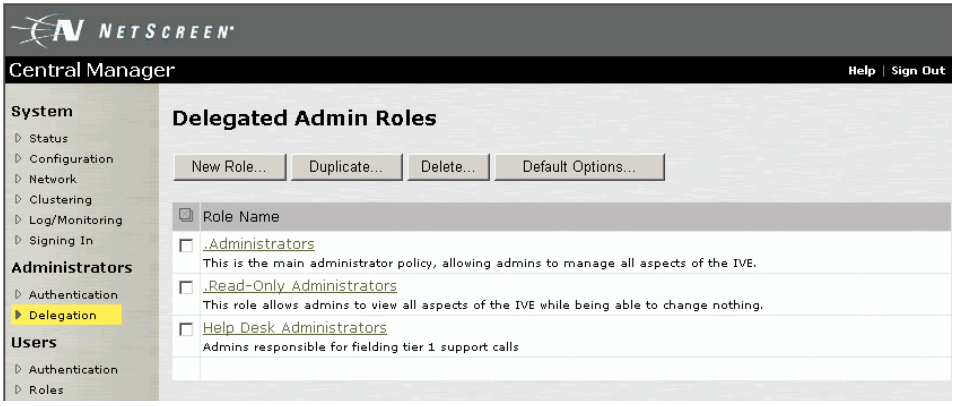


Abbildung 67: Administrators > Delegation

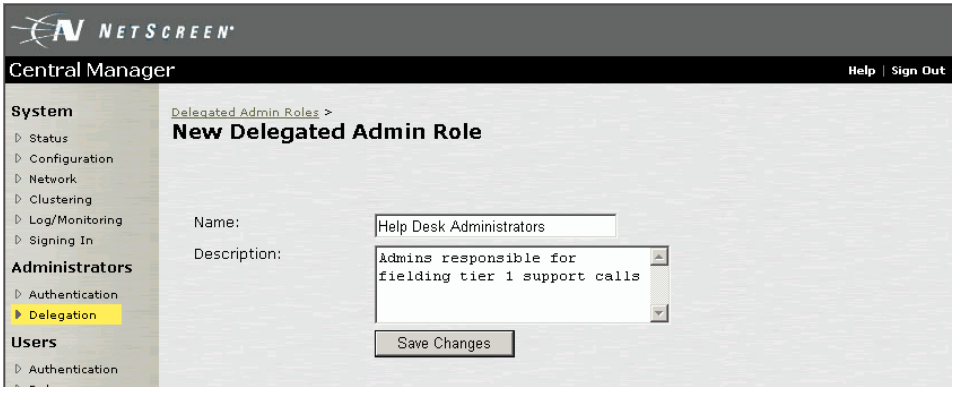


Abbildung 68: Administrators > Delegation > New Role

Registerkarte „General“

☑ Konfigurieren allgemeiner Einstellungen für eine Administratorrolle

Auf dieser Registerkarte können Sie Quell-IP-Einschränkungen, Browsereinschränkungen, Zertifikateinschränkungen, Hostprüfungseinschränkungen, Sitzungsoptionen und UI-Optionen für delegierte Administratorrollen konfigurieren. Weitere Informationen zu den Optionen auf diesen Registerkarten finden Sie unter „Registerkarte „General > Overview““ auf Seite 286.

Registerkarte „System“

☑ Delegieren von Verwaltungsaufgaben an eine Administratorrolle

Auf dieser Registerkarte können Sie IVE-Verwaltungsaufgaben an verschiedene Administratorrollen delegieren. Beachten Sie beim Delegieren von Berechtigungen, dass alle Administratoren (mindestens) über Lesezugriff auf die Webkonsole-Startseite (**System > Status > Overview**) verfügen, unabhängig von der ausgewählten Berechtigungsebene.

Beachten Sie auch, dass delegierte Administratoren keinen Schreibzugriff auf Seiten haben, auf denen Sie ihre eigenen Berechtigungen ändern können. Nur die systemintegrierten Administratorrollen (**.Administrators** und **.Read-Only Administrators**) dürfen auf diese Seiten zugreifen:

- System > Signing In
- Administrators > Authentication
- Administrators > Delegation
- Users > Authentication
- Users > New User
- Maintenance > Import/Export (**.Read-Only Administrators** können Einstellungen in dieser Seite exportieren, jedoch nicht importieren.)
- Maintenance > Push Config
- Maintenance > Archiving > Local Backups

So legen Sie Administrationsberechtigungen für eine Administratorrolle fest:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **System**.
4. Geben Sie für jede Hauptkategorie (**System tasks**, **Maintenance tasks**, **Resource policies** und **Users**) die für die Rolle zulässige Zugriffsebene an. Jede Hauptkategorie entspricht direkt Optionen in der Webkonsole.
   - **Deny All** – Gibt an, dass Mitglieder der Administratorrolle keine Einstellungen in der Kategorie anzeigen oder ändern können.
   - **Read All** – Gibt an, dass Mitglieder der Administratorrolle Einstellungen in der Kategorie anzeigen, aber nicht ändern können.
   - **Read All** – Gibt an, dass Mitglieder der Administratorrolle alle Einstellungen in der Kategorie ändern können.
   - **Custom Settings** – Ermöglicht Ihnen die Auswahl von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für die einzelnen Funktionen innerhalb der Kategorie.
5. Klicken Sie auf **Save Changes**.

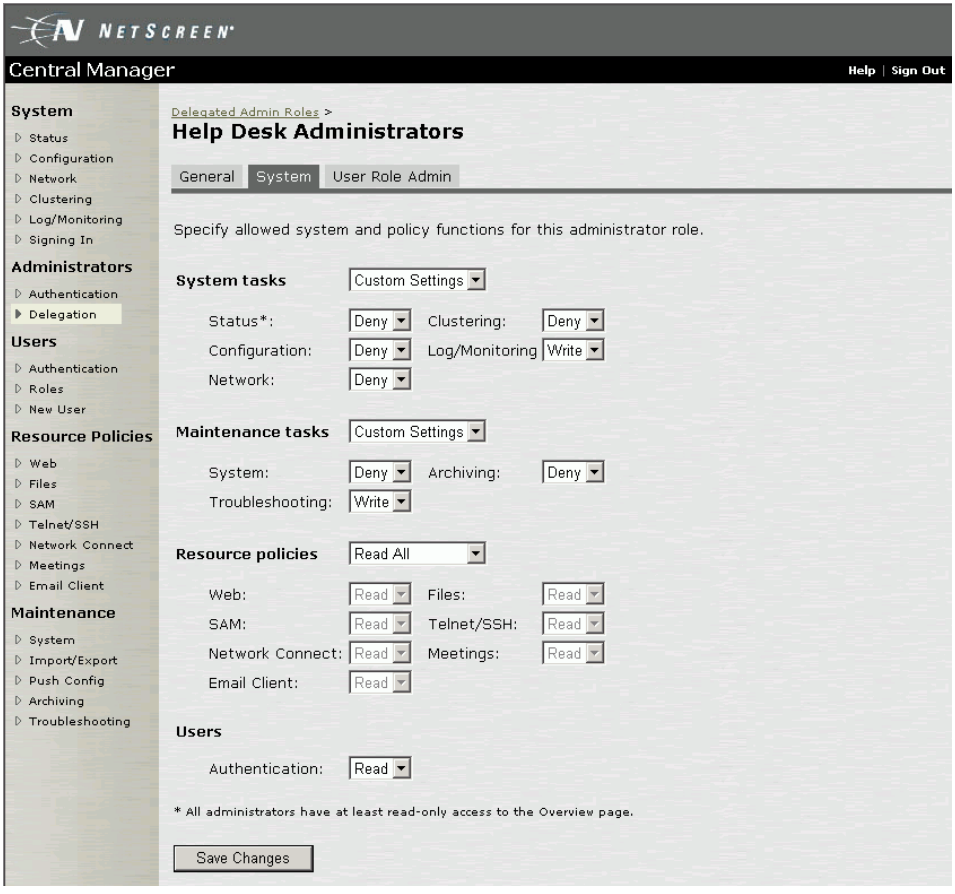


Abbildung 69: Administrators > Delegation > [Ausgewählte Rolle] > System

Registerkarte „User Role Admin“

☑ Delegieren von Benutzerrollenverwaltung an eine Administratorrolle

Auf dieser Registerkarte können Sie die Benutzerrollen angeben, die von einer Administratorrolle verwaltet werden können. Beachten Sie beim Delegieren von Rollenverwaltungsberechtigungen Folgendes:

- Wenn Sie dem delegierten Administrator für alle Funktionen innerhalb einer Benutzerrolle Lese- und Schreibzugriff gewähren, gestattet das IVE dem delegierten Administrator auch Lesezugriff auf die Webkonsole-Startseite für diese Benutzerrolle (**User > Role > [Rolle] > General > Overview**).
- Das IVE deaktiviert für alle delegierten Administratoren die Befehle **New Role**, **Duplicate** und **Delete** auf der Seite **User > Roles**.
- Wenn Sie einem delegierten Administrator über die Seite **Administrators > Delegation > [Administratorrolle] > System** Schreibzugriff auf eine Ressourcenrichtlinie erteilen, kann er eine Ressourcenrichtlinie erstellen, die auf alle Benutzerrollen anwendbar ist, auch wenn er nicht über Lesezugriff auf diese Rolle verfügt.

So definieren Sie Rollenverwaltungsberechtigungen für eine Administratorrolle:

1. Wählen Sie in der Webkonsole **Administrators > Delegation** aus.
2. Wählen Sie die Administratorrolle aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **User Role Admin**.
4. Wählen Sie unter **Allowed Roles** die Benutzerrollen aus, deren Verwaltung Sie dem Administrator erlauben möchten.
5. Geben Sie unter **Permissions** die dem Administrator ermöglichte Zugriffsebene an:
   - **Write All** – Gibt an, dass Mitglieder der Administratorrolle alle Einstellungen für die ausgewählte(n) Benutzerrolle(n) ändern können.
   - **Custom Settings** – Ermöglicht Ihnen die Auswahl von Administratorberechtigungen (**Deny**, **Read** oder **Write**) für die einzelnen Funktionen innerhalb der Benutzerrolle.
6. Wählen Sie unter **Read-only roles** die Benutzerrollen aus, die der Administrator anzeigen, nicht jedoch verwalten darf.
7. Klicken Sie auf **Save Changes**.

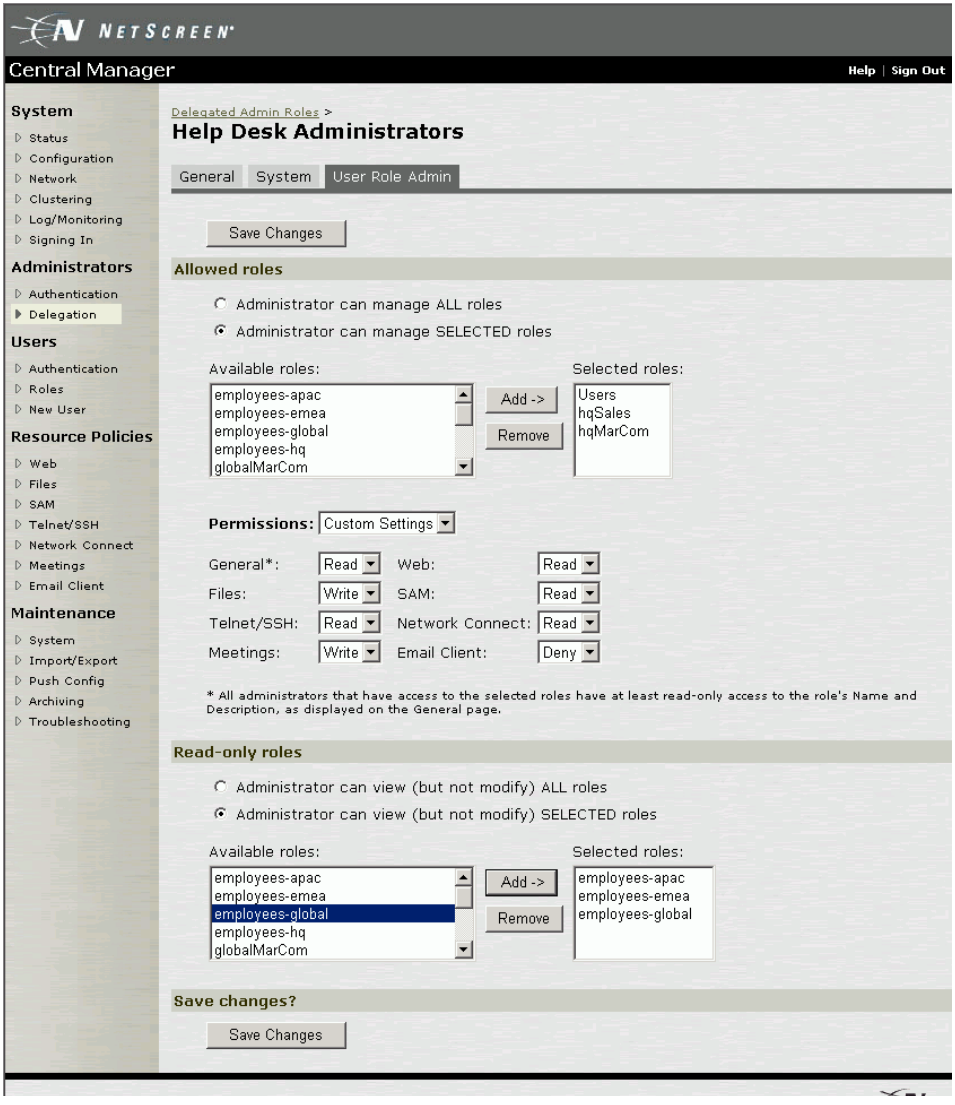


Abbildung 70: Administrators > Delegation > [Ausgewählte Rolle] > User Role Admin

Konfigurieren eines Authentifizierungsbereichs

Über die Menüs **Administrators > Authentication** und **Users > Authentication** können Benutzer auf die entsprechenden Seiten für **Authentication Realms** zugreifen. Auf diesen Seiten können Sie Authentifizierungsbereiche im System erstellen und verwalten.

Die Seite **Authentication Realms** enthält die folgenden Registerkarten:

Registerkarte „General“ 273
Registerkarte „Authentication Policy“ 275
Registerkarte „Role Mapping“ 277

Auf den Registerkarten der Seite **Authentication Realms** können Sie Folgendes durchführen:

Erstellen eines Authentifizierungsbereichs 273
Angeben einer Richtlinie für einen Authentifizierungsbereich 275
Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich 277
Use the server catalog 279

Registerkarte „General“

Auf der Registerkarte **General** können Sie einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 35.

☑ Erstellen eines Authentifizierungsbereichs

So erstellen Sie einen Authentifizierungsbereich:

1. Wählen Sie in der Webkonsole **Administrators > Authentication** oder **Users > Authentication** aus.
2. Klicken Sie auf der entsprechenden Seite **Authentication Realms** auf **New Realm**.
3. Verfahren Sie auf der Seite **New Realm** folgendermaßen:
   1. Geben Sie eine Bezeichnung für diesen Bereich ein.
   2. Geben Sie eine Beschreibung für den Bereich ein. (Optional.)
   3. Aktivieren Sie **When editing, start on the Role Mapping page**, wenn die Registerkarte **Role Mapping** beim Öffnen des Bereichs zur Bearbeitung aktiviert sein soll.

4. Legen Sie unter **Servers** Folgendes fest:
   - Einen Authentifizierungsserver, der zum Authentifizieren von Benutzern verwendet werden soll, die sich bei diesem Bereich anmelden.
   - Einen Verzeichnis-/Attributserver zum Abrufen von Benutzerattributen und Gruppeninformationen für Rollenzuordnungsregeln und Ressourcenrichtlinien. (Optional.)
5. Klicken Sie auf **Save Changes**, um den Bereich auf dem IVE zu erstellen. Die Registerkarten **General**, **Authentication Policy** und **Role Mapping** für den Authentifizierungsbereich werden angezeigt.
6. Führen Sie die nächsten Konfigurationsschritte aus:
   1 Konfigurieren Sie mindestens eine Rollenzuordnungsregel. (Seite 277)
   2 Konfigurieren Sie eine Authentifizierungsrichtlinie für den Bereich. (Seite 275)

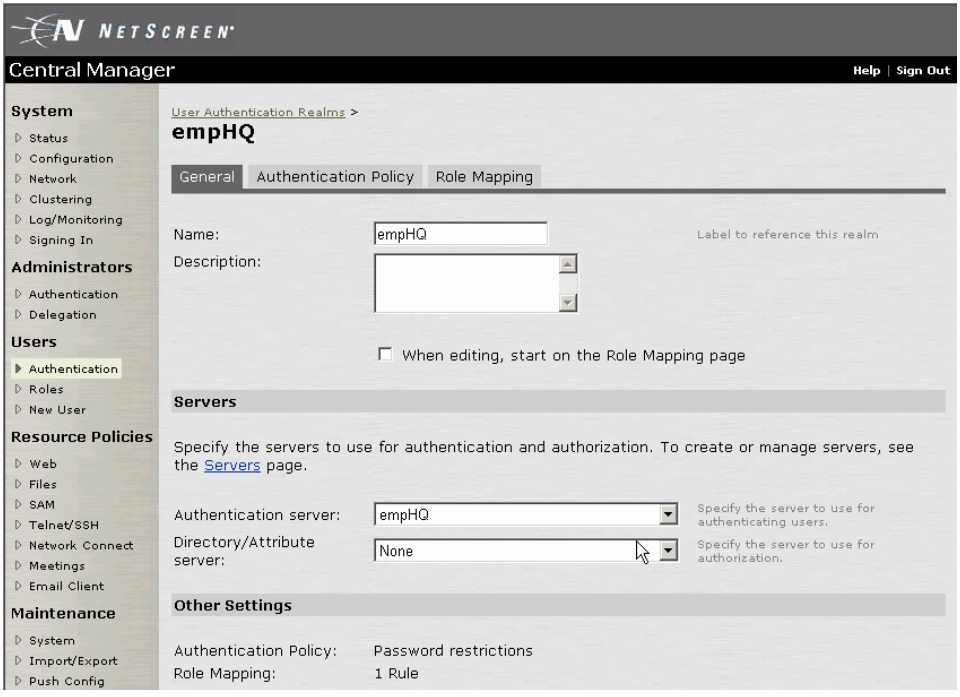


Abbildung 71: Users | Administrators > Authentication > *Bereichsname* > General

Registerkarte „Authentication Policy“

Auf der Registerkarte **Authentication Policy** können Sie eine Richtlinie für einen Authentifizierungsbereich erstellen. Weitere Informationen zu Bereichen finden Sie unter „Authentifizierungsbereiche – Übersicht“ auf Seite 35.

☑ Angeben einer Richtlinie für einen Authentifizierungsbereich

So geben Sie eine Richtlinie für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole **Administrators > Authentication** oder **Users > Authentication** aus.
2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Authentication Policy**.
3. Konfigurieren Sie auf der Seite **Authentication Policy** mindestens eine der folgenden Zugriffsverwaltungsoptionen:
   - Quell-IP (Seite 428)
   - Browser (Seite 429)
   - Zertifikat (Seite 432)
   - Kennwort (Seite 433)
   - Hostprüfung (Seite 434)
   - Cachebereinigung (Seite 435) *Nur in Benutzerbereichen verfügbar.*
   - Begrenzungen (Seite 428)

Begrenzungen für gleichzeitig angemeldete Benutzer

Neben den Zugriffsverwaltungsoptionen, die Sie für eine Authentifizierungsrichtlinie festlegen können, können Sie auch die Höchstanzahl gleichzeitig angemeldeter Benutzer festlegen. Konfigurieren Sie diese Einstellung hier:

- Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits
- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Limits

Nur wenn ein Benutzer, der in einer der Anmeldeseiten dieses Bereichs einen URL eingibt, alle Benutzeranforderungen hinsichtlich Zugriffsverwaltung und gleichzeitig angemeldeter Benutzer erfüllen, die für die Authentifizierungsrichtlinie festgelegt sind, wird vom IVE eine Anmeldeseite geöffnet.

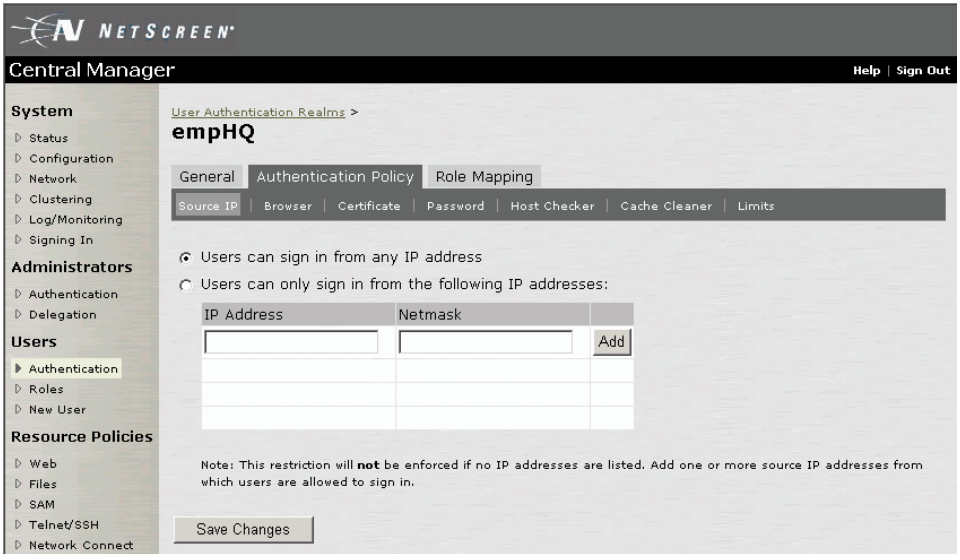


Abbildung 72: Users | Administrators > Authentication > *Bereichsname* > Authentication Policy

Registerkarte „Role Mapping“

Auf der Registerkarte **Role Mapping** können Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich festlegen. Entsprechende Informationen finden Sie auf folgenden Seiten:

- Bereiche siehe „Authentifizierungsbereiche – Übersicht“ auf Seite 35.
- Rollen siehe „Benutzerrollen – Übersicht“ auf Seite 55.

☑ Angeben von Rollenzuordnungsregeln für einen Authentifizierungsbereich

Zum Erstellen einer neuen Regel, die LDAP-Benutzerattribute, LDAP-Gruppeninformationen oder benutzerdefinierte Ausdrücke verwendet, müssen Sie den Serverkatalog verwenden. Informationen zu diesem Katalog finden Sie unter „Use the server catalog“ auf Seite 279.

So geben Sie Rollenzuordnungsregeln für einen Authentifizierungsbereich an:

1. Wählen Sie in der Webkonsole **Administrators > Authentication** oder **Users > Authentication** aus.
2. Wählen Sie auf der entsprechenden Seite **Authentication Realms** einen Bereich aus, und klicken Sie dann auf die Registerkarte **Role Mapping**.
3. Klicken Sie auf **New Rule**, um auf die Seite **Role Mapping Rule** zuzugreifen. Diese Seite stellt einen integrierten Editor für die Definition von Regeln bereit.
4. Wählen Sie in der Liste **Rule based on** eins der folgenden Elemente aus:
   - **Benutzername**

     Benutzername ist der IVE-Benutzername, der auf der Anmeldeseite eingegeben wird. Wählen Sie diese Option aus, wenn Benutzer anhand ihrer IVE-Benutzernamen zu Rollen zugeordnet werden sollen. Dieser Regeltyp ist für alle Bereiche verfügbar.

   - **Benutzerattribut**

     Benutzerattribut ist ein Benutzerattribut, das entweder aus einem RADIUS- oder einem LDAP-Server stammt. Wählen Sie diese Option aus, wenn Benutzer anhand eines Attributs vom entsprechenden Server zu Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen RADIUS-Server als Authentifzierungsserver oder einen LDAP-Server als Authentifizierungs- bzw. Verzeichnisserver verwenden.

- **Certificate** oder **Certificate attribute**

  Certificate oder *Certificate attribute* ist ein Attribut, das vom clientseitigen Zertifikat des Benutzers unterstützt wird. Wählen Sie diese Option aus, wenn Benutzer anhand ihrer Zertifikatsattribute zu Rollen zugeordnet werden sollen. Die Option *Certificate* ist für alle Bereiche verfügbar, während die Option *Certificate attribute* nur für Bereiche verfügbar ist, die einen LDAP-Authentifizierungs- oder Verzeichnisserver verwenden.

- **Group membership**

  Group membership ist eine Angabe zur Gruppe von einem LDAP-Server, die Sie zur Registerkarte **Groups** des Serverkatalogs hinzufügen. Wählen Sie diese Option aus, wenn Benutzer anhand der LDAP-Gruppeninformationen zu Rollen zugeordnet werden sollen. Dieser Regeltyp steht nur für Bereiche zur Verfügung, die einen LDAP-Server als Authentifizierungs- oder Verzeichnisserver benutzen.

- **Custom Expressions**

  Custom Expressions sind benutzerdefinierte Ausdrücke, die Sie im Serverkatalog definieren. Wählen Sie diese Option aus, wenn Benutzer anhand benutzerdefinierter Ausdrücke zu Rollen zugeordnet werden sollen. Dieser Regeltyp ist für alle Bereiche verfügbar.

5. Geben Sie unter **Rule** die auszuwertende Bedingung an, die dem ausgewählten Regeltyp entspricht und folgende Punkte umfasst:
   1. Angeben von mindestens einem Benutzernamen, einem RADIUS- oder LDAP-Benutzerattribut, einem Zertifikatsattribut, einer LDAP-Gruppe oder einem benutzerdefinierten Ausdruck.
   2. Angeben der Wertentsprechungen. Dies kann auch eine Liste von IVE-Benutzernamen, Benutzerattributswerten von einem RADIUS- oder LDAP-Server, clientseitigen Zertifikatswerten (statische oder LDAP-Attribute), LDAP-Gruppen oder benutzerdefinierten Ausdrücken umfassen.
6. Nehmen Sie unter **...then assign these roles** folgende Eingaben vor:
   1. Geben Sie die Rollen an, die Sie dem authentifizierten Benutzer zuordnen wollen, indem Sie Rollen zur Liste **Selected Roles** hinzufügen.
   2. Aktivieren Sie die Option **Stop processing rules when this rule matches**, wenn das IVE die Auswertung der Rollenzuordnungsregeln anhalten soll, wenn der Benutzer die für diese Regel angegebenen Bedingungen erfüllt.

7. Klicken Sie auf **Save Changes**, um die Regel auf der Registerkarte **Role Mapping** zu erstellen. Gehen Sie nach dem Abschluss der Regelerstellung folgendermaßen vor:
   - Bringen Sie die Regeln unbedingt in die Reihenfolge, in der das IVE diese auswerten soll. Diese ist besonders dann wichtig, wenn die Verarbeitung der Rollenzuordnungsregeln bei einer Übereinstimmung angehalten werden soll.
   - Geben Sie an, ob die Einstellungen für alle zugeordneten Rollen zusammengeführt werden sollen. Weitere Informationen finden Sie unter „Richtlinien für permissive Zusammenführungen“ auf Seite 59.

Abbildung 73: Users | Administrators > Authentication > *Bereichsname* > Role Mapping

☑ Use the server catalog

Der ***Server Catalog*** ist ein sekundäres Fenster, in dem Sie Zusatzinformationen angeben können, die das IVE für die Zuordnung von Benutzern zu Rollen verwendet, darunter:

- **Attributes**

  Auf der Registerkarte **Server Catalog Attributes** wird eine Liste von allgemeinen LDAP-Attributen angezeigt, z. B. `cn`, `uid`, `uniquemember` und `memberof`. Diese Registerkarte kann nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden. Auf dieser

Registerkarte können Sie die Attribute eines LDAP-Servers verwalten, indem Sie seinem IVE-Serverkatalog benutzerdefinierte Werte hinzufügen oder Werte aus diesem löschen. Beachten Sie, dass das IVE eine lokale Kopie der LDAP-Serverwerte aufbewahrt. Attribute werden dem Wörterbuch weder hinzugefügt noch aus diesem gelöscht.

- **Groups**

  Über die Registerkarte **Server Catalog Groups** können Gruppeninformationen einfach von einem LDAP-Server abgefragt und dem Serverkatalog eines IVE-Servers hinzugefügt werden. Sie geben den BaseDN der Gruppen und ggf. einen Filter an, um die Suche zu starten. Wenn Ihnen der genaue Container der Gruppen nicht bekannt ist, können Sie den Domänenstamm als BaseDN festlegen, z.B. `dc=netscreen, dc=com`. Die Suchseite gibt eine Gruppenliste vom Server zurück, aus der Sie Gruppen auswählen können, die in die Liste **Groups** eingegeben werden.

  Hinweis: Der auf der Konfigurationsseite des LDAP-Servers unter „Finding user entries“ angegebene BaseDN-Wert ist der Standard-BaseDN-Wert. Der Filterwert ist standardmäßig auf (cn=*) gesetzt.

  Sie können Gruppen auch auf der Registerkarte **Groups** angeben. Sie müssen den FQDN (Fully Qualified Distinguished Name) einer Gruppe angeben, z.B. cn=Manager, ou=Zentrale, ou=NetScreen, o=com, c=DE, können dieser Gruppe jedoch eine Bezeichnung zuordnen, die in der Liste **Groups** angezeigt wird. Beachten Sie, dass diese Registerkarte nur beim Zugriff auf den Serverkatalog eines LDAP-Servers aufgerufen werden kann.

- **Expressions**

  Auf der Registerkarte **Server Catalog Expressions** können Sie benutzerdefinierte Ausdrücke für die Rollenzuordnungsregel schreiben.

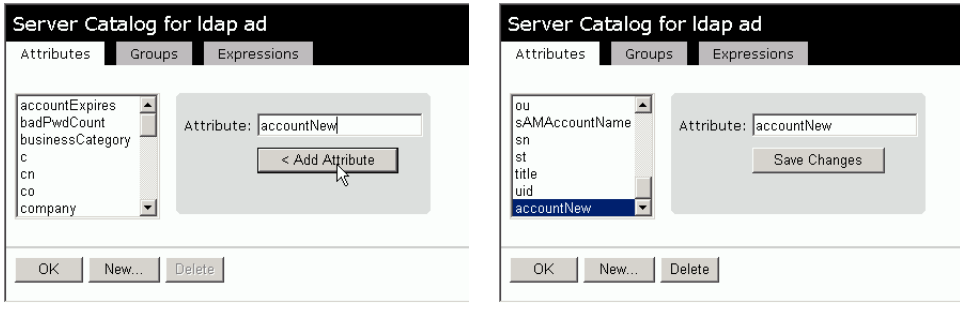


Abbildung 74: Registerkarte „Server Catalog Attributes“ – Hinzufügen eines Attributs

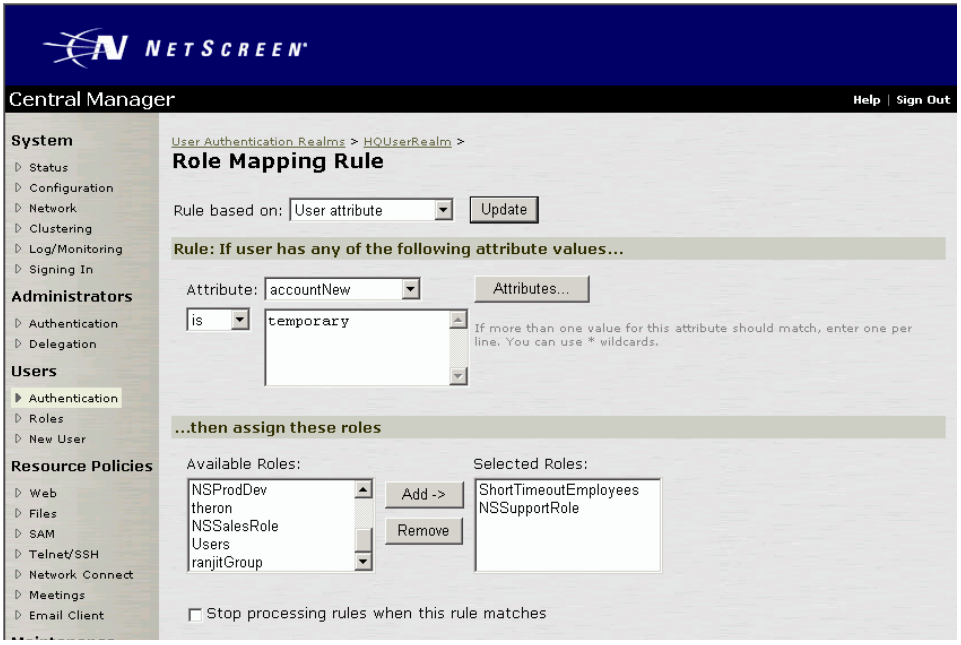


Abbildung 75: Das im Serverkatalog hinzugefügte Attribut steht für die Rollenzuordnungsregel zur Verfügung

Abbildung 76: Registerkarte „Server Catalog Groups“ – Hinzufügen einer LDAP-Gruppe

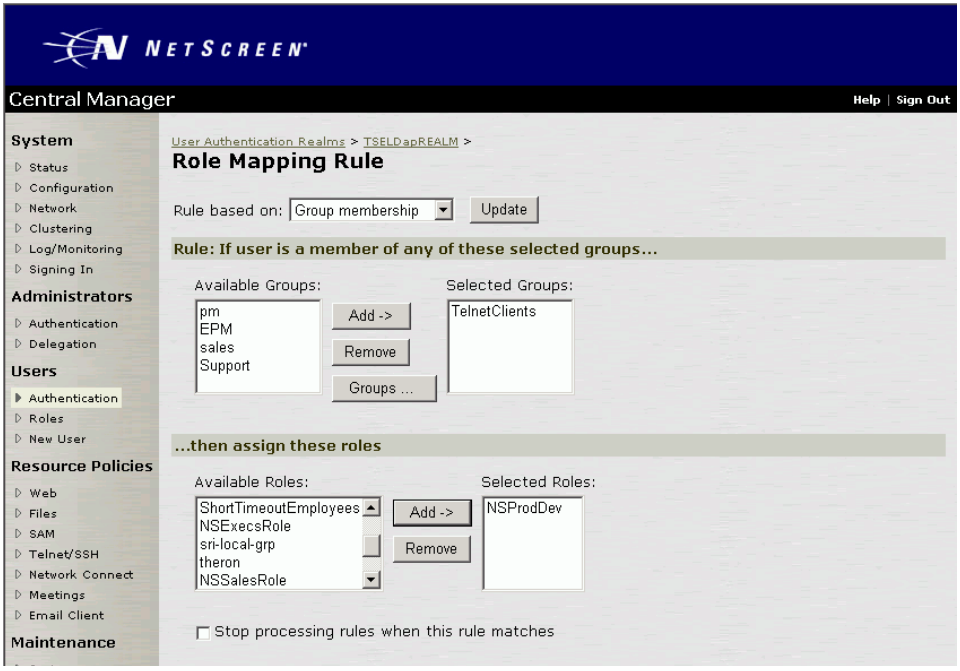


Abbildung 77: Die im Serverkatalog hinzugefügte Gruppe steht für die Rollenzuordnungsregel zur Verfügung

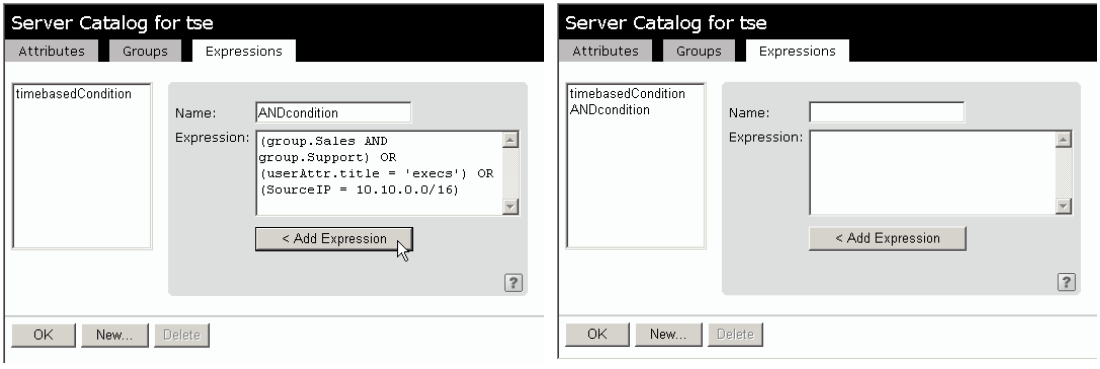


Abbildung 78: Registerkarte „Server Catalog Expressions“ – Hinzufügen eines benutzerdefinierten Ausdrucks

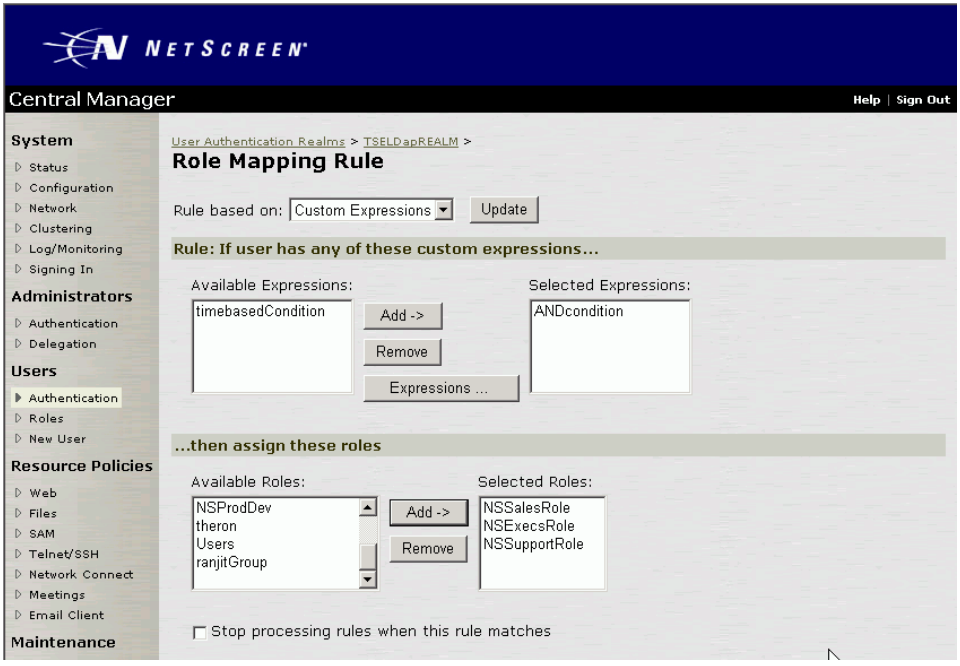


Abbildung 79: Der im Serverkatalog hinzugefügte benutzerdefinierte Ausdruck steht für die Rollenzuordnungsregel zu Verfügung

Konfigurieren der Seite „Roles“

Benutzer können über das Menü **Users > Roles** auf die Seiten **Roles** zugreifen. Auf dieser Seite können Sie Benutzerrollen im System erstellen und verwalten. Klicken Sie zum Erstellen einer Rolle auf **New Role**, und geben Sie dann einen Namen sowie bei Bedarf eine Beschreibung ein. Dieser Name wird auf der Seite **Roles** in der Liste **Roles** angezeigt. Klicken Sie auf den Namen der Rolle, um auf den Registerkarten für Rollen mit der Konfiguration zu beginnen.

Die Seite **Users > Roles** enthält die folgenden Registerkarten:

Registerkarte „General > Overview“ 286
Registerkarte „General > Restrictions“ 287
Registerkarte „General > Session Options“ 289
Registerkarte „General > UI Options“ 293
Registerkarte „Web > Bookmarks“ 294
Registerkarte „Web > Options“ 296
Registerkarte „Files > Windows Bookmarks“ 299
Registerkarte „Files > UNIX Bookmarks“ 301
Registerkarte „Files > Options“ 302
Registerkarte „SAM > Applications“ 304
Registerkarte „SAM > Options“ 312
Registerkarte „Telnet/SSH > Sessions“ 315
Registerkarte „Telnet/SSH > Options“ 316
Registerkarte „Meetings“ 317
Registerkarte „Network Connect“ 322

Auf den Registerkarten der Seite **Users > Roles** können Sie Folgendes durchführen:

Verwalten allgemeiner Einstellungen und Optionen für Rollen 286
Festlegen von Zugriffsverwaltungsoptionen für die Rolle 288
Angeben der Einstellungen für Benutzersitzungszeiten, Roaming, Beständigkeit und Anforderungen 289
Anpassen der IVE-Willkommensseite für Benutzer mit Rollen 293
Erstellen von Lesezeichen für Webressourcen 295
Angeben von allgemeinen Webbrowsingoptionen 296
Erstellen von Lesezeichen für Windows-Ressourcen 299
Erstellen von Lesezeichen für UNIX-Ressourcen 301
Angeben von allgemeinen Optionen zum Navigieren durch Dateien 302
Angeben von Anwendungen und Servern, die mit W-SAM gesichert werden sollen 305

Angeben von Anwendungen, die mit J-SAM gesichert werden sollen 306
Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich) 310
Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt 311
Angeben allgemeiner Optionen für Secure Application Manager 312
Erstellen von Lesezeichen für sichere Terminalsitzungen 315
Angeben allgemeiner Optionen für Telnet/SSH 316
Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen 318
Festlegen der Option für das lokale Subnetz von Network Connect 322

Registerkarte „General > Overview“

Auf der Registerkarte **General > Overview** können Sie den Namen und die Beschreibung von Rollen bearbeiten, Sitzungs- und Benutzeroberflächenoptionen an- und ausschalten sowie Zugriffsfunktionen aktivieren. Wenn Sie eine Zugriffsfunktion aktivieren, müssen Sie auch entsprechende Ressourcenrichtlinien erstellen.

☑ Verwalten allgemeiner Einstellungen und Optionen für Rollen

So verwalten Sie allgemeine Einstellungen und Optionen für Rollen:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> General > Overview** aus.
2. Überprüfen Sie den Namen und die Beschreibung, und klicken Sie anschließend auf **Save Changes**. (Optional.)
3. Aktivieren Sie unter **Options** folgende Kontrollkästchen:
   - **Session Options**, um die auf der Registerkarte **General > Session Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
   - **UI Options**, um die auf der Registerkarte **General > UI Options** konfigurierten Einstellungen auf die Rolle anzuwenden.
4. Aktivieren Sie unter **Access features** die für die Rolle vorgesehenen Funktionen. Folgende Optionen stehen zur Verfügung: Web, Dateien, Secure Application Manager (Windows- oder JAVAVERSION), Telnet/SSH, Konferenzen, E-Mail-Client und Network Connect.
5. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

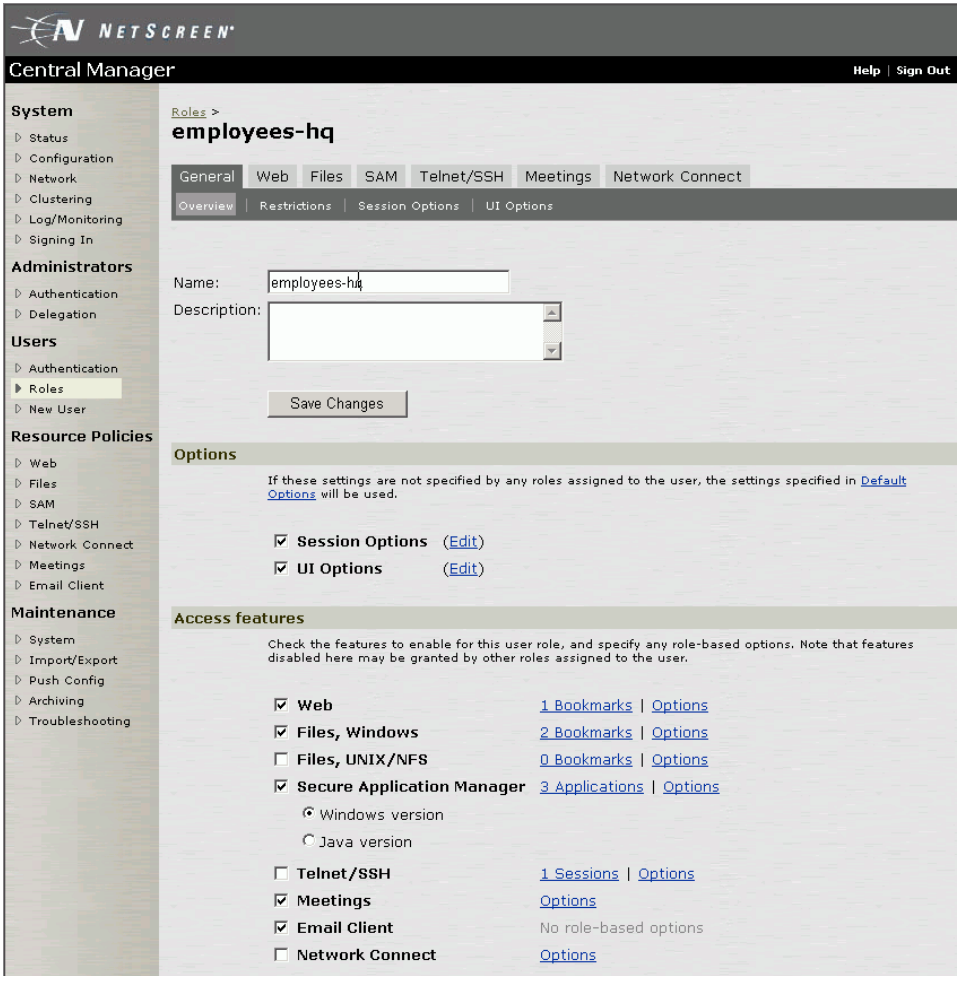


Abbildung 80: Users > Roles > *Ausgewählte Rolle* > General > Overview

Registerkarte „General > Restrictions“

Legen Sie auf der Registerkarte **General > Restrictions** Zugriffsverwaltungsoptionen für die Rolle fest. Das IVE berücksichtigt diese Beschränkungen, wenn es ermittelt, ob ein Benutzer einer Rolle zugeordnet wird. Benutzer werden der Rolle vom IVE nur dann zugeordnet, wenn Sie die angegebenen Beschränkungen erfüllen. Weitere Informationen zur Zugriffsverwaltung finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 23.

☑ Festlegen von Zugriffsverwaltungsoptionen für die Rolle

So legen Sie Zugriffsverwaltungsoptionen für die Rolle fest:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> General > Restrictions** aus.
2. Klicken Sie auf die Registerkarte, die der Option entspricht, die Sie für die Rolle konfigurieren möchten:
   - Source IP (Seite 428)
   - Browser (Seite 429)
   - Certificate (Seite 432)
   - Host Checker (Seite 434)
   - Cache Cleaner (Seite 435)

   Für die Rolle kann eine beliebige Anzahl von Zugriffsverwaltungsoptionen konfiguriert werden. Wenn ein Benutzer nicht alle Beschränkungen erfüllt, ordnet das IVE ihn der Rolle nicht zu.

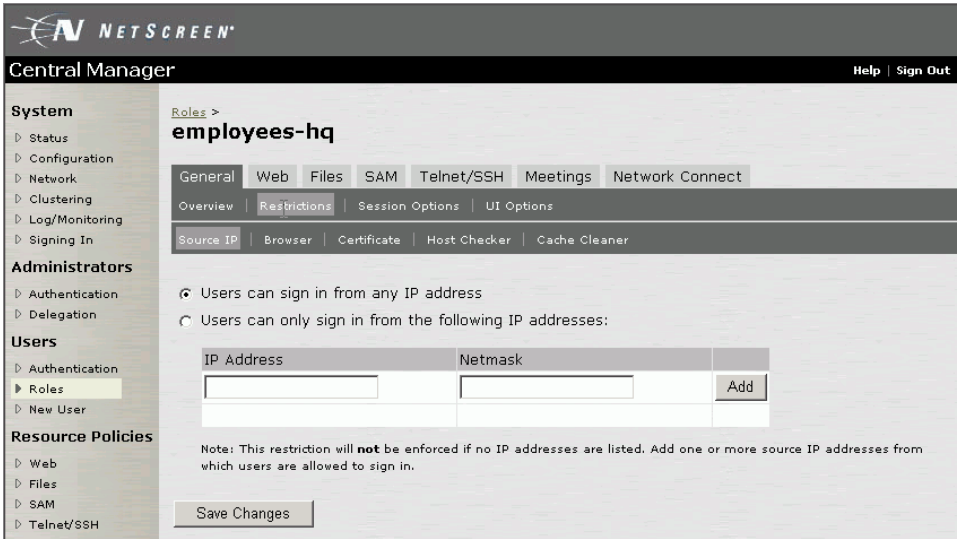


Abbildung 81: Users > Roles > *Ausgewählte Rolle* > General > Restrictions

Registerkarte „General > Session Options“

Auf der Registerkarte **General > Session** können Sie Sitzungszeitbegrenzungen, Roamingfunktionen, die Sitzungs- und Kennwortbeständigkeit sowie Optionen zur Anforderungsverfolgung festlegen. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Session Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ Angeben der Einstellungen für Benutzersitzungszeiten, Roaming, Beständigkeit und Anforderungen

So geben Sie allgemeine Sitzungsoptionen an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> General > Session Options** aus.
2. Geben Sie unter **Session Lifetime** Werte für folgende Optionen an:
   - **Idle Timeout** – Geben Sie die Anzahl der Minuten an, die sich eine nicht administrative Benutzersitzung im Leerlauf befinden kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Leerlaufzeitbegrenzung für Sitzungen beträgt in der Standardeinstellung zehn Minuten, d.h., eine Benutzersitzung, die zehn Minuten lang inaktiv ist, wird vom IVE beendet, und das Ereignis wird im Systemprotokoll protokolliert (sofern Sie nicht die unten beschriebenen Warnungen bei Sitzungszeitüberschreitung aktivieren).
   - **Max. Session Length** – Geben Sie die Anzahl der Minuten an, die eine aktive nicht administrative Benutzersitzung geöffnet bleiben kann, bevor sie beendet wird. Die Mindestzeit beträgt drei Minuten. Die Standardzeitbegrenzung für eine Benutzersitzung beträgt sechzig Minuten. Nach dieser Zeitspanne beendet das IVE die Benutzersitzung und protokolliert das Ereignis im Systemprotokoll.
   - **Reminder Time** – Geben Sie den Zeitpunkt an, zu dem das IVE Benutzer (außer Administratoren) wegen einer bevorstehenden Sitzungs- oder Leerlaufzeitüberschreitung warnen soll. Geben Sie die Anzahl von Minuten vor Erreichen der Überschreitung an.
3. Aktivieren Sie unter **Enable Session timeout warning** das Optionsfeld **Enabled**, um vor dem Erreichen der Sitzungszeitbegrenzung oder des Leerlaufzeitlimits auch andere Benutzer als Administratoren zu benachrichtigen. In diesen Warnungen werden Benutzer aufgefordert, kurz vor Erreichen der Sitzungsbegrenzung oder des Leerlaufzeitlimits eine geeignete Aktion durchzuführen, um gerade in Verarbeitung befindliche Formulardaten speichern zu können, die andernfalls verloren gehen würden. Benutzer, die sich dem Leerlaufzeitlimit nähern, werden

zum Reaktivieren der Sitzung aufgefordert. Benutzer, die sich der Sitzungszeitbegrenzung nähern, werden zum Speichern der Daten aufgefordert.

Ein IVE-Benutzer kann zum Beispiel bei der Arbeit mit einem für die Zusammenarbeit mit dem IVE konfigurierten E-Mail-Client unwissentlich das Leerlaufzeitlimit für seine Autorisierungsgruppe erreichen, da das IVE während des Verfassens der E-Mail keine Daten empfängt. Wenn Warnungen bei Sitzungszeitüberschreitung aktiviert sind, fordert das IVE den Benutzer jedoch auf, die IVE-Sitzung vor Ablauf der Zeitbegrenzung zu reaktivieren und erzwingt das Beenden der IVE-Sitzung des Benutzers. Diese Warnung gibt dem Benutzer die Möglichkeit, die teilweise verfasste E-Mail zu speichern.

4. Geben Sie unter **Roaming session** Folgendes an:
   - **Enabled** – Ermöglicht Roamingbenutzersitzungen für Benutzer, die dieser Gruppe zugeordnet sind. Eine Roamingbenutzersitzung funktioniert über Quell-IP-Adressen, wodurch sich mobile Benutzer (Benutzer von Laptops) mit dynamischen IP-Adressen von einem Standort aus im IVE anmelden können und Ihre Arbeit von einem anderen Standort fortsetzen können. Einige Browser weisen jedoch eventuell Schwachstellen auf, über die durch bösartigen Code Benutzercookies gestohlen werden können. Ein böswilliger Benutzer kann dann anhand eines gestohlenen IVE-Sitzungscookies am IVE anmelden.
   - **Limit to subnet** – Beschränkt die Roamingsitzung auf das lokale Subnetz, das im Feld **Netmask** angegeben ist. Benutzer können sich von einer IP-Adresse aus anmelden und ihre Sitzungen mit einer anderen IP-Adresse fortsetzen, sofern sich die neue IP-Adresse in demselben Subnetz befindet.
   - **Disabled** – Verbietet Roamingbenutzersitzungen für Benutzer, die dieser Rolle zugeordnet sind. Benutzer, die sich von einer IP-Adresse aus anmelden, können eine aktive IVE-Sitzung nicht von einer anderen IP-Adresse aus fortsetzen. Benutzersitzungen sind an die ursprüngliche Quell-IP-Adresse gebunden.
5. Aktivieren Sie unter **Persistent session** das Optionsfeld **Enabled**, um das IVE-Sitzungscookie auf die Festplatte des Clients zu schreiben, sodass die Anmeldeinformationen des IVE-Benutzers für die Dauer der IVE-Sitzung gespeichert werden.

   Standardmäßig wird das IVE-Sitzungscookie aus dem Speicher des Browsers gelöscht, wenn der Browser geschlossen wird. Die IVE-Sitzungsdauer wird sowohl vom Wert des Leerlaufzeitlimits als auch dem Wert der Höchstsitzungsdauer bestimmt, die Sie für die Rolle angeben. Die IVE-Sitzung wird nicht beendet, wenn ein Benutzer den Browser schließt. Eine IVE-Sitzung wird erst dann beendet, wenn sich ein Benutzer vom IVE abmeldet. Wenn ein Benutzer das Browserfenster

schließt, ohne sich abzumelden, kann jeder beliebige Benutzer eine andere Instanz desselben Browsers öffnen, um auf das IVE zuzugreifen, ohne gültige Anmeldeinformationen zu senden.

Hinweis: Wir empfehlen, diese Funktion nur für Rollen zu aktivieren, deren Mitglieder den Zugriff auf Anwendungen benötigen, für die IVE-Anmeldeinformationen erforderlich sind. Zudem sollten Sie dafür sorgen, dass sich diese Benutzer der Bedeutung der Abmeldung vom IVE nach Abschluss der Sitzung bewusst sind.

---

6. Aktivieren Sie unter **Persistent password caching** das Optionsfeld **Enabled**, damit zwischengespeicherte Kennwörter über mehrere Sitzungen für eine Gruppe erhalten bleiben können.

   Der IVE unterstützt die NTLM- und HTTP-Standardauthentifizierung sowie Server, die sowohl für NTLM-Anmeldungen als auch für anonyme Anmeldungen eingerichtet sind. Das IVE speichert von Benutzern eingegebene Kennwörter für die NTLM- und HTTP-Standardauthentifizierung im Cache, sodass die Benutzer nicht wiederholt aufgefordert werden, die Anmeldeinformationen einzugeben, die bereits bei der Anmeldung beim IVE-Server oder einer anderen Ressource in der NT-Domäne verwendet wurden. Standardmäßig leert der IVE-Server zwischengespeicherte Kennwörter aus dem Cache, wenn sich ein Benutzer abmeldet. Ein Benutzer kann zwischengespeicherte Kennwörter über die Seite **Advanced Preferences** löschen.

7. Aktivieren Sie unter **Browser request follow-through** das Optionsfeld **Enabled**, sodass Benutzeranforderungen vom IVE verarbeitet werden können, die nach Ablauf einer Benutzersitzung und erneuter Authentifizierung des Benutzers vorgenommen wurden.

8. Klicken Sie auf **Save Changes**, um die Einstellungen auf die Rolle anzuwenden.

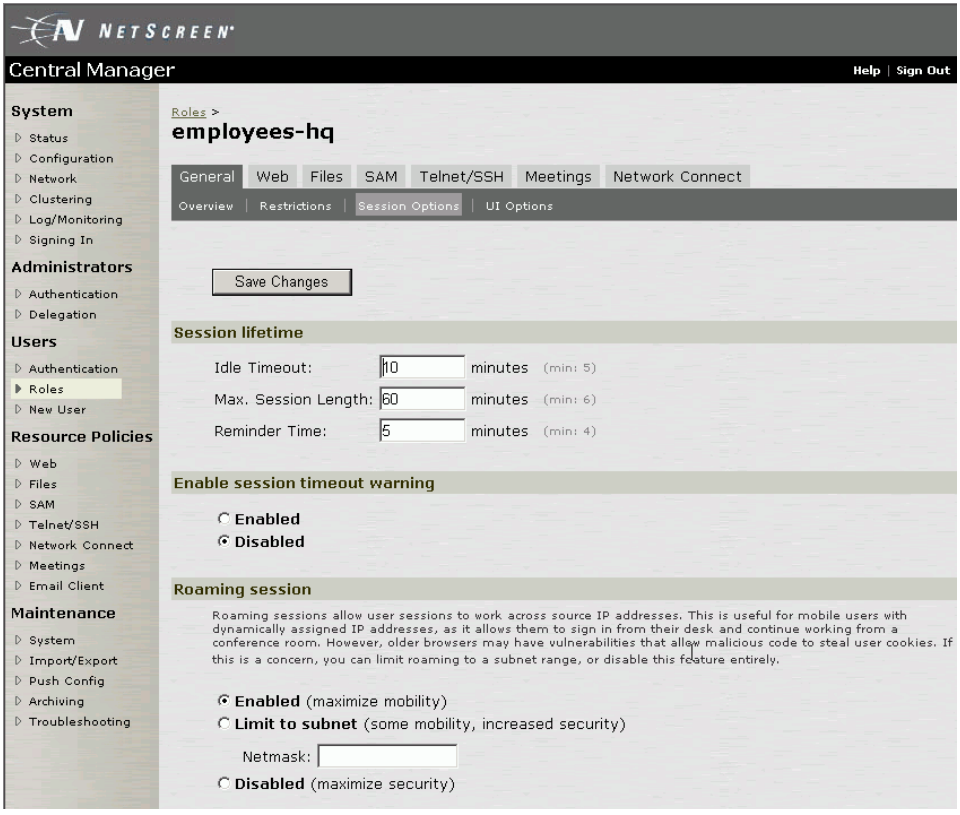


Abbildung 82: Users > Roles > *Ausgewählte Rolle* > General > Session Options

Registerkarte „General > UI Options“

Auf der Registerkarte **General > UI Options** können Sie benutzerdefinierte Einstellungen für die IVE-Willkommensseite angeben, die dieser Rolle zugeordneten Benutzern angezeigt wird. Die IVE-Willkommensseite (oder Startseite) ist die Weboberfläche, die authentifizierten IVE-Benutzern angezeigt wird. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **UI Options**, um diese Einstellungen für die Rolle zu aktivieren.

☑ Anpassen der IVE-Willkommensseite für Benutzer mit Rollen

So passen Sie die IVE-Willkommensseite für Benutzer mit Rollen an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> General > UI Options** aus.
2. Ändern Sie in den Abschnitten **Custom Text** und **Custom Error Messages** den für die verschiedenen Fenstertitel verwendeten Standardtext nach Bedarf.
3. Legen Sie im Abschnitt **Header** eine benutzerdefinierte Logobilddatei und eine andere Farbe für den Seitenkopf fest.
4. Um Benutzern benutzerdefinierte Hilfeinformationen oder zusätzliche Anweisungen bereitzustellen, wählen Sie **Show Help Button**, geben Sie eine Beschriftung für die Schaltfläche ein, und legen Sie eine HTML-Datei fest, die in das IVE hochgeladen werden soll. Beachten Sie, dass im IVE keine Bilder und anderen Inhalte angezeigt werden, auf die auf dieser HTML-Seite verwiesen wird.
5. Klicken Sie auf **Save Changes**. Die Änderungen werden sofort wirksam, doch möglicherweise muss bei den aktuellen Browsersitzungen von Benutzern eine Aktualisierung durchgeführt werden, damit die Änderungen angezeigt werden.
6. Klicken Sie auf **Restore Factory Defaults**, um die Darstellung der Anmeldeseite, der IVE-Startseite für Benutzer und der Webkonsole zurückzusetzen.

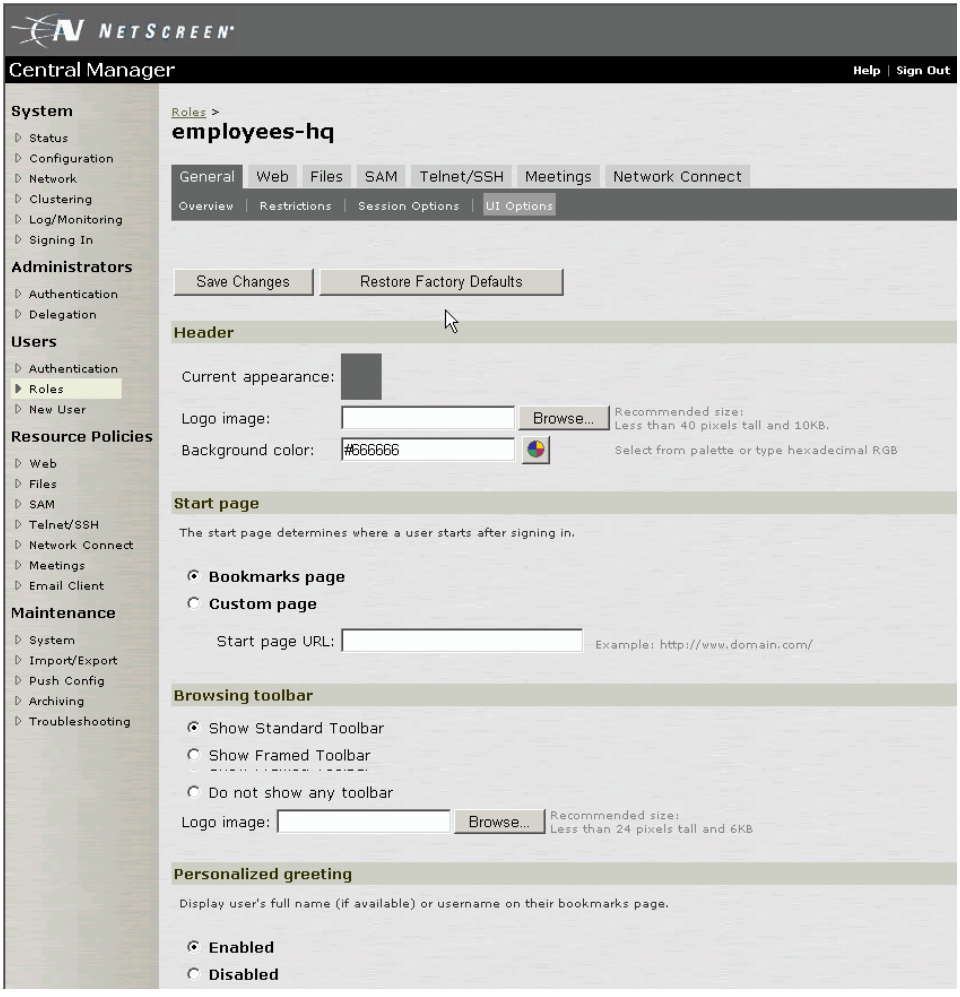


Abbildung 83: Users > Roles > *Ausgewählte Rolle* > General > UI Options

Registerkarte „Web > Bookmarks“

Auf der Registerkarte **Web > Bookmarks** können Sie Weblesezeichen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. Sie können den IVE-Benutzernamen eines Benutzers im URL-Pfad einfügen, um bei Einzelanmeldung den Zugriff auf Back-End-Webanwendungen zu ermöglichen.

☑ Erstellen von Lesezeichen für Webressourcen

So erstellen Sie ein Lesezeichen für eine Webressource:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Web > Bookmarks** aus.
2. Klicken Sie auf **New Bookmark**, und geben Sie dann die erforderlichen Informationen ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im URL <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des URLs auf der IVE-Startseite angezeigt.
3. Klicken Sie auf **Save** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

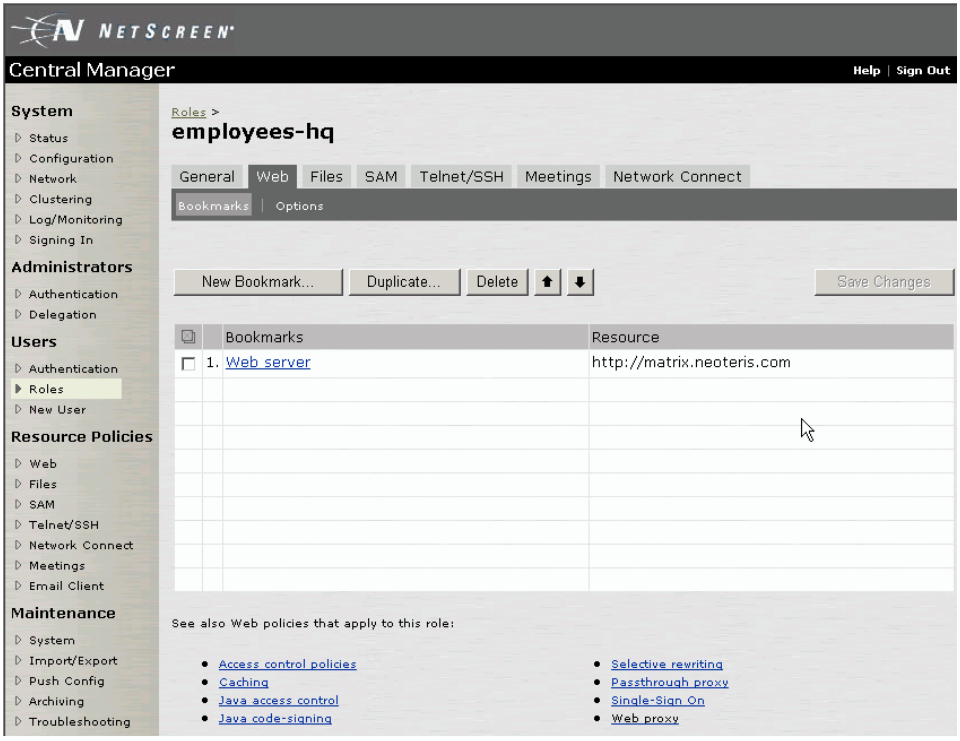


Abbildung 84: **Users > Roles >** ***Ausgewählte Rolle*** **> Web > Bookmarks**

Registerkarte „Web > Options“

Auf der Registerkarte **Web > Options** können Sie allgemeine Webbrowsingoptionen festlegen.

☑ Angeben von allgemeinen Webbrowsingoptionen

So geben Sie allgemeine Webbrowsingoptionen an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Web > Options** aus.
2. Geben Sie unter **Browsing** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can type URLs** – Diese Option ermöglicht es Benutzern, auf der Willkommensseite URLs einzugeben und zu Sites im Internet zu navigieren.
   - **Allow Java applets** – Diese Option ermöglicht es Benutzern, zu Webseiten zu navigieren, die clientseitige Java-Applets enthalten. Der IVE-Server wird für den Anwendungsserver wie ein Browser über SSL behandelt. Das IVE verarbeitet alle durch ein Java-Applet initiierten HTTP-Anforderungen und TCP-Verbindungen transparent und verarbeitet signierte Java-Applets.

     Wenn Sie diese Funktion aktivieren, können die Benutzer Java-Applets starten und Anwendungen ausführen, die als clientseitige Java-Applets implementiert wurden, z. B. VNC-Java-Client (Virtual Computing), Citrix NFuse Java-Client, WRQ Reflections Web-Client und Lotus WebMail. Diese Funktion wird zusammen mit den Ressourcenrichtlinien für die Java-Codesignatur verwendet.
   - **Mask hostnames while browsing** – Diese Option ermöglicht es Benutzern, Zielressouren im URL zu verbergen, die von Benutzern aufgerufen werden können. Wenn Sie die Option auswählen, werden die IP-Adressen und Hostnamen für den Benutzer an folgenden Stellen maskiert:
     - Adressleiste des Webbrowsers (wenn der Benutzer eine Seite aufruft)
     - Statusleiste des Webbrowsers (beim Führen des Mauszeigers über einen Hyperlink)
     - HTML-Quelldateien (wenn der Benutzer „View Source“ auswählt)
     - Die Hostnamencodierung verhindert, dass sich zufällige Besucher den URL einer internen Ressource notieren können, da der Zielserver im URL verborgen wird, ohne dabei den vollständigen Pfadname, die Zieldatei oder die Portnummer zu maskieren. Wenn ein Benutzer beispielsweise „www.msn.com“ aufruft, ohne dass

selektives Neuschreiben oder Hostnamencodierung aktiviert ist, wird der folgende URL in der Adressleiste des Webbrowsers des Benutzers angezeigt: http://www.msn.com/

- **Unrewritten pages open in new window** – Wenn Benutzer auf Seiten zugreifen, die nicht neu geschrieben werden (siehe Seite „Selective Rewriting policy"), erzwingt diese Option, dass der Inhalt in einem neuen Fenster angezeigt wird. So werden Benutzer daran erinnert, dass sie sich noch immer in einer sicheren Sitzung befinden.

3. Geben Sie unter **Bookmarks** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, auf der IVE-Willkommensseite persönliche Weblesezeichen zu erstellen.
   - **Auto-allow role bookmarks** – Diese Option ermöglicht es dem IVE, für diese Rolle automatisch ein Weblesezeichen für die Ressourcenrichtlinien für Webzugriff zu erstellen. Beachten Sie, dass diese Funktion nur für Rollenlesezeichen, nicht für von Benutzern erstellte Lesezeichen gilt.
4. Aktivieren Sie unter **Cookies** die Option **Persistent cookies**, sodass Benutzer, die dieser Rolle angehören, ihre Browserumgebung durch Beibehaltung beständiger Cookies anpassen können. Standardmäßig löscht das IVE Webcookies, die während einer Benutzersitzung gespeichert wurden. Bei Aktivierung dieser Option können Benutzer Cookies über die Seite **Advanced Preferences** löschen.
5. Klicken Sie auf **Save Changes**.

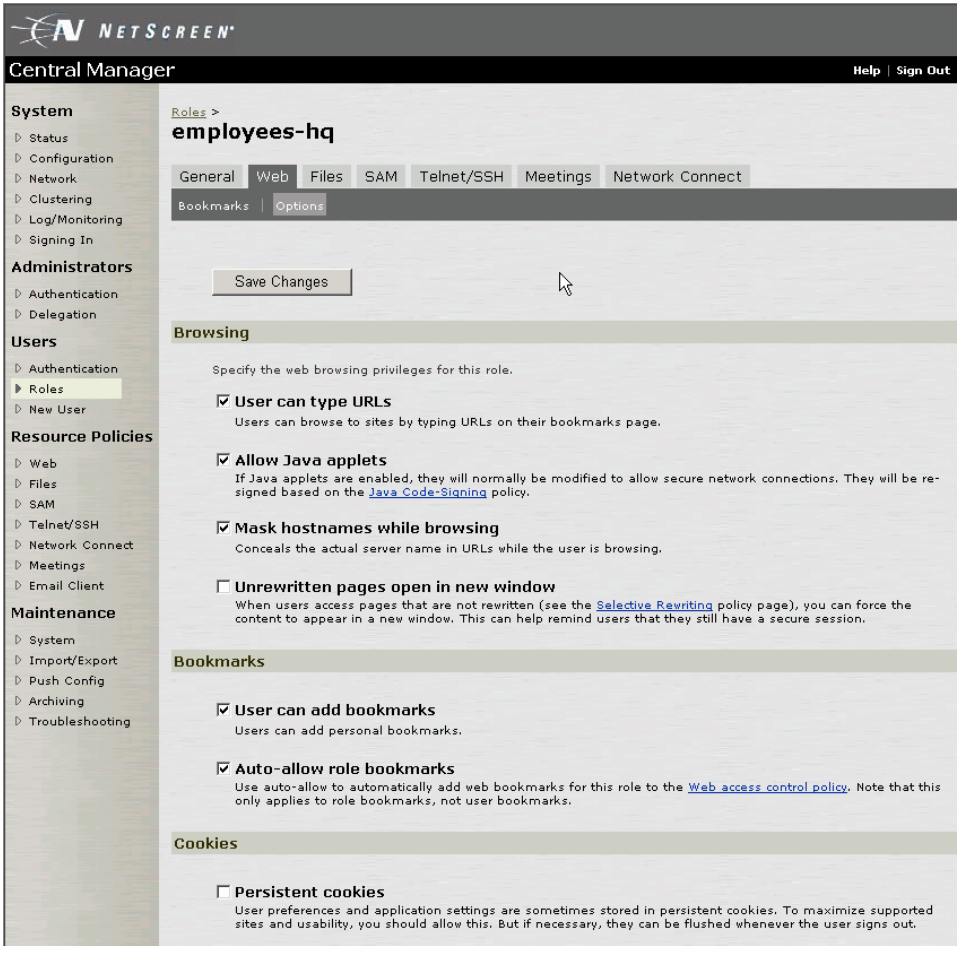

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
employees-hq
General
Web
Files
SAM
Telnet/SSH
Meetings
Network Connect
Bookmarks
Options
Save Changes
Browsing
Specify the web browsing privileges for this role.
User can type URLs
Users can browse to sites by typing URLs on their bookmarks page.
Allow Java applets
If Java applets are enabled, they will normally be modified to allow secure network connections. They will be re-signed based on the Java Code-Signing policy.
Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing.
Unrewritten pages open in new window
When users access pages that are not rewritten (see the Selective Rewriting policy page), you can force the content to appear in a new window. This can help remind users that they still have a secure session.
Bookmarks
User can add bookmarks
Users can add personal bookmarks.
Auto-allow role bookmarks
Use auto-allow to automatically add web bookmarks for this role to the Web access control policy. Note that this only applies to role bookmarks, not user bookmarks.
Cookies
Persistent cookies
User preferences and application settings are sometimes stored in persistent cookies. To maximize supported sites and usability, you should allow this. But if necessary, they can be flushed whenever the user signs out.

Abbildung 85: Users > Roles > *Ausgewählte Rolle* > Web > Options

Registerkarte „Files > Windows Bookmarks“

Auf der Registerkarte **Files > Windows Bookmarks** können Sie Windows-Lesezeichen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

Wenn IVE-Benutzer zu Dateien auf einem Dfs-Server navigieren, gibt der Dfs-Server anhand der in Active Directory gespeicherten Site-Konfigurationsdaten Dfs-Verweise in der richtigen Reihenfolge an das IVE zurück. Verweise auf nähere Servers befinden sich in der Liste an einer höheren Position als Verweise auf weiter entfernte Server. Die Clients durchlaufen die Verweise in der Reihenfolge, in der diese empfangen werden. Wenn eine Anforderung von einem Client eingeht, der sich in einem nicht in der Liste aufgeführten Subnetz befindet, besitzt der Server keine Informationen über den Standort des Clients und gibt die Verweise in zufälliger Reihenfolge zurück. Auf diese Weise greifen Dfs-Anforderungen vom IVE (in diesem Falle in der Rolle des Clients) möglicherweise auf einen wesentlich weiter entfernten Server zu. Dies wiederum kann zu erheblichen Verzögerungen führen, insbesondere wenn das IVE versucht, auf einen Server zuzugreifen, der aus dem Subnetz mit dem IVE nicht erreichbar ist. Wenn das IVE in einem Subnetz installiert ist, das sich nicht in der Liste des Dfs-Servers befindet, kann der Dfs-Administrator das Subnetz mit dem IVE auf dem Domänencontroller mit dem Tool „Active Directory-Standorte und -Dienste“ zur entsprechenden Site hinzufügen.

☑ Erstellen von Lesezeichen für Windows-Ressourcen

So erstellen Sie ein Lesezeichen für eine Windows-Ressource:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Files > Windows Bookmarks** aus.
2. Klicken Sie auf **New Bookmark** , und wechseln Sie dann zum Server und Freigabenamen, bzw. geben Sie diesen ein. Geben Sie einen Pfad ein, um den Zugriff weiter einzuschränken. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/der Freigabe auf der IVE-Startseite angezeigt.

Hinweis: Ein Windows-Server kann nicht mit einem Lesezeichen versehen werden. Sie müssen sowohl den Server- als auch den Freigabenamen angeben.

---

3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:
   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.
4. Geben Sie für **Access** Folgendes an:
   - **Enable auto-allow access to this bookmark** – Das IVE erstellt für die Windows-Zugriffsressourcenrichtlinie automatisch ein Lesezeichen für diese Rolle. Diese Funktion gilt nur für Rollenlesezeichen, nicht für Lesezeichen, die von Benutzern erstellt wurden. Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können.
   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.
5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

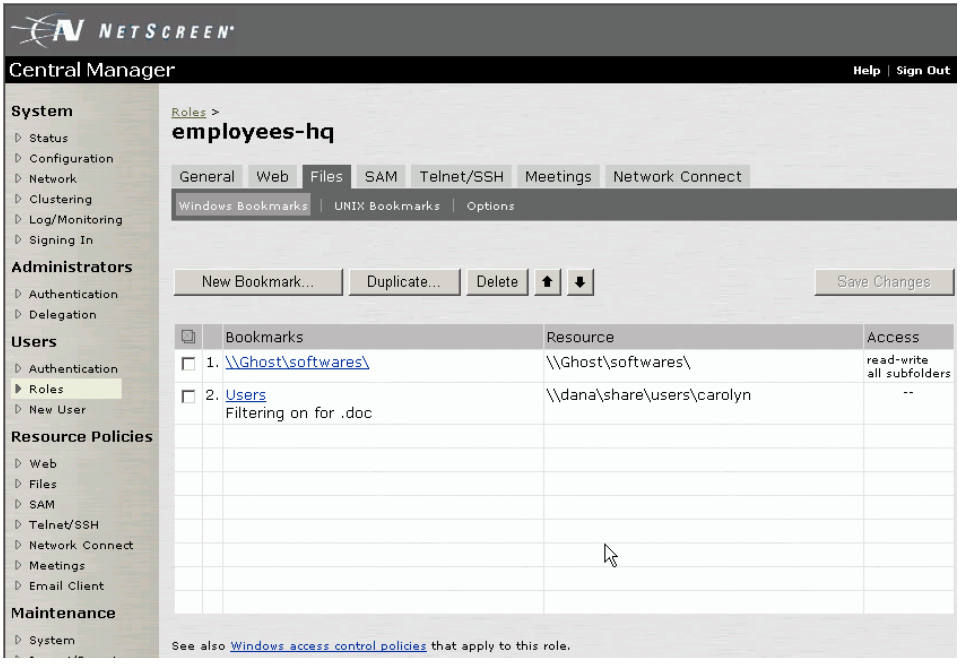


Abbildung 86: Users > Roles > *Ausgewählte Rolle* > Files > Windows Bookmarks

Registerkarte „Files > UNIX Bookmarks“

Auf der Registerkarte **Files > UNIX Bookmarks** können Sie UNIX/NFS-Lesezeichen erstellen, die auf der IVE-Startseite angezeigt werden. Sie können den IVE-Benutzernamen des Benutzers in den URL-Pfad einfügen, um so einen schnellen Zugriff auf die Netzwerkverzeichnisse des Benutzers zu ermöglichen.

☑ Erstellen von Lesezeichen für UNIX-Ressourcen

So erstellen Sie ein Lesezeichen für eine UNIX/NFS-Ressource:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Files > UNIX Bookmarks** aus.
2. Klicken Sie auf **New Bookmark** , und geben Sie den Hostnamen oder die IP-Adresse des Servers und den Pfad zu der Freigabe ein. Wenn Sie den Benutzernamen des Benutzers einfügen möchten, geben Sie an der entsprechenden Stelle im Pfad <USER> (in Großbuchstaben) ein. Wenn Sie einen Namen und eine Beschreibung für das Lesezeichen angeben, werden diese Informationen anstelle des Servers/Pfades auf der IVE-Startseite angezeigt.
3. Wählen Sie für **Appearance** eine der folgenden Optionen aus:
   - **Appear as bookmark on homepage and in file browsing** – Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Appear in file browsing only** – Das Lesezeichen wird dem Benutzer nur beim Navigieren durch Netzwerkdateien angezeigt.
4. Geben Sie für **Access** Folgendes an:
   - **Enable auto-allow access to this bookmark** – Das IVE erstellt für die Windows-Zugriffsressourcenrichtlinie automatisch ein Lesezeichen für diese Rolle. Diese Funktion gilt nur für Rollenlesezeichen, nicht für Lesezeichen, die von Benutzern erstellt wurden. Das Lesezeichen wird dem Benutzer sowohl auf der Willkommensseite als auch beim Navigieren durch Netzwerkdateien angezeigt.
   - **Read-write access**, damit Benutzer Dateien auf dem Server speichern können.
   - **Include sub-folders**, damit Benutzer Dateien in den Verzeichnissen unter dem angegebenen Lesezeichenpfad anzeigen können.
5. Klicken Sie auf **Save Changes** oder **Save + New**, um ein weiteres Lesezeichen hinzuzufügen.

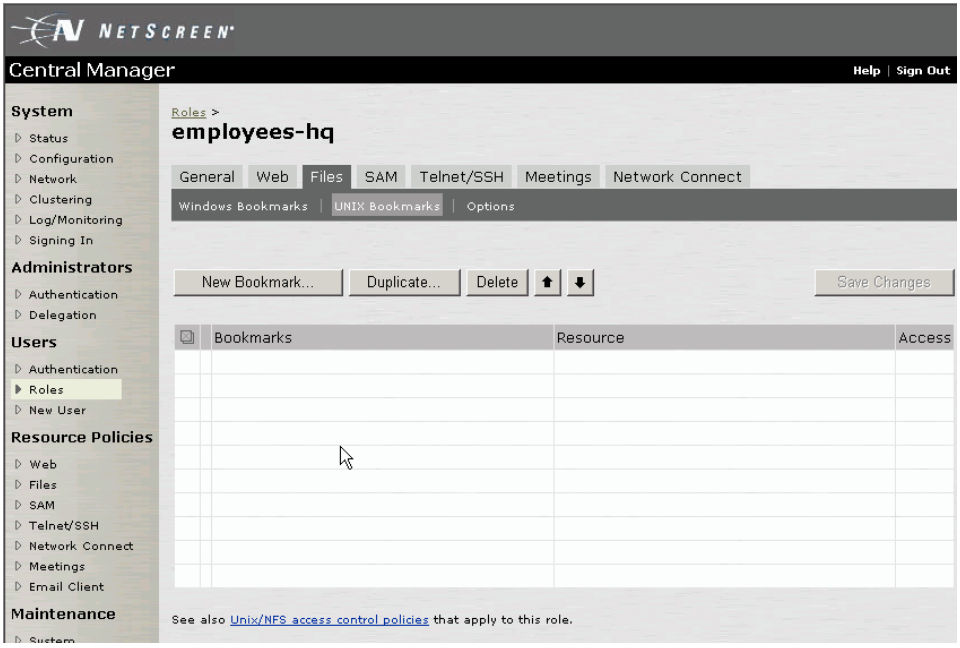


Abbildung 87: Users > Roles > *Ausgewählte Rolle* > Files > UNIX Bookmarks

Registerkarte „Files > Options“

Auf der Registerkarte **Files > Options** können Sie die Optionen zum Navigieren in Windows- und UNIX/NFS-Netzwerken angeben, einschließlich der Möglichkeit, Ressourcen anzuzeigen und Ordnerlesezeichen zu erstellen. Diese Optionen werden zusammen mit den Dateiressourcenrichtlinien verwendet.

☑ Angeben von allgemeinen Optionen zum Navigieren durch Dateien

So geben Sie allgemeine Optionen für die Dateinavigation an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Web > Options** aus.
2. Geben Sie unter **Windows Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.

- **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.

3. Geben Sie unter **UNIX Network Files** die Optionen an, die für Benutzer aktiviert werden sollen:
   - **User can browse network file shares** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren UNIX-Dateifreigaben anzuzeigen und zu erstellen.
   - **User can add bookmarks** – Diese Option ermöglicht es Benutzern, Lesezeichen für Ressourcen in verfügbaren Windows-Dateifreigaben anzuzeigen und zu erstellen.
   - **Allow automount shares** – Diese Option ermöglicht es Benutzern, auf Automount-Freigaben zuzugreifen, die auf einem NIS-Server angegeben sind.
4. Klicken Sie auf **Save Changes**.

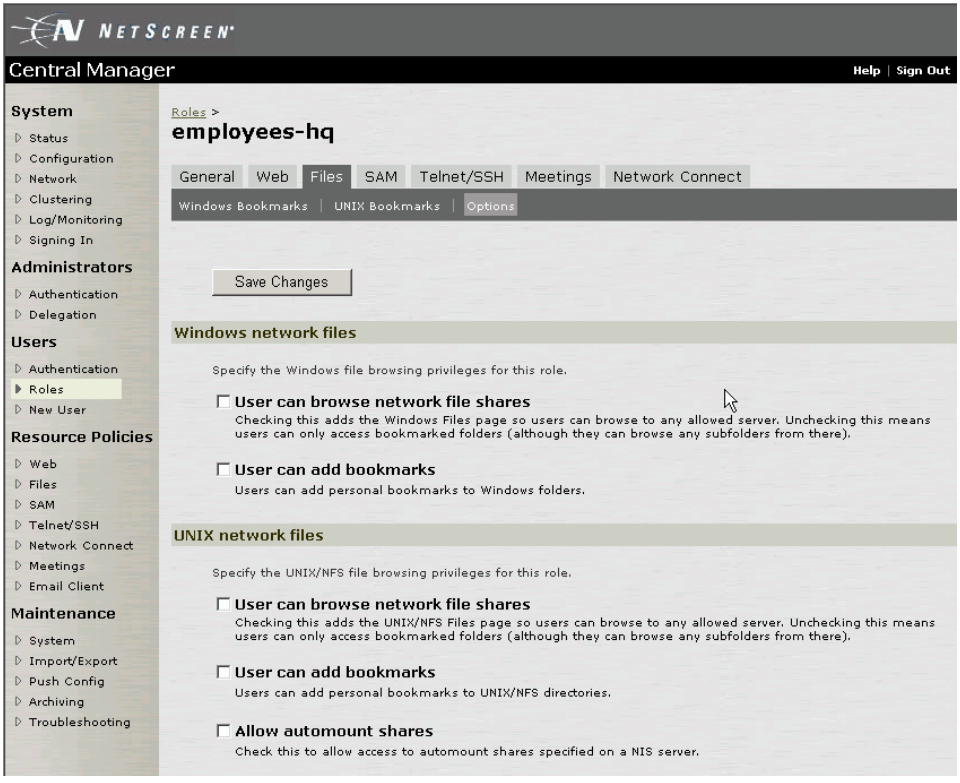


Abbildung 88: Users > Roles > *Ausgewählte Rolle* > Files > Options

Registerkarte „SAM > Applications“

Auf der Registerkarte **SAM > Applications** können Sie Client/Server-Anwendungen angeben, die von Secure Application Manager vermittelt werden sollen. Auf dieser Registerkarte werden je nach SAM-Version, die für die Rolle aktiviert ist, unterschiedliche Optionen angezeigt. Bei Aktivierung von:

- W-SAM, siehe „Angeben von Anwendungen und Servern, die mit W-SAM gesichert werden sollen“ auf Seite 305
- J-SAM, siehe „Angeben von Anwendungen und Servern, die mit W-SAM gesichert werden sollen“ auf Seite 305

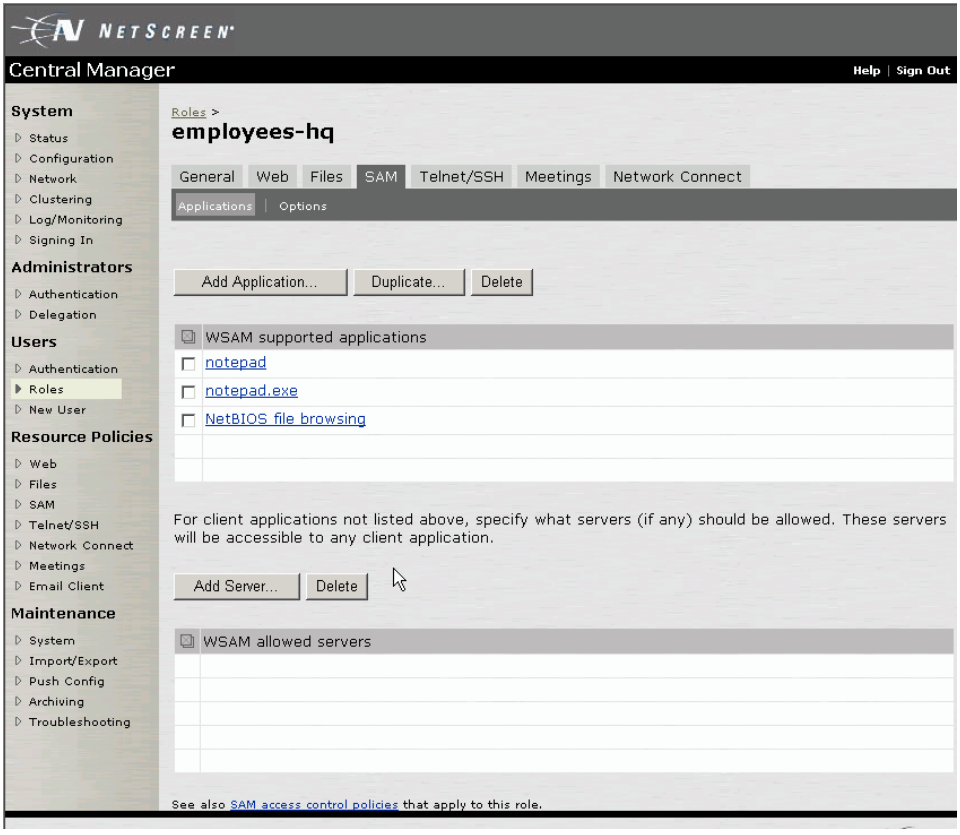


Abbildung 89: Users > Roles > *Ausgewählte Rolle* > SAM > Applications

☑ Angeben von Anwendungen und Servern, die mit W-SAM gesichert werden sollen

Auf der Registerkarte **Applications** können Sie Anwendungen und Server festlegen, für die W-SAM den Datenverkehr sichert. Wenn W-SAM auf einen Client-PC heruntergeladen wird, enthält dieser Informationen, die Sie für die Rolle auf der Registerkarte **Applications** konfiguriert haben. Nachdem ein Benutzer Secure Application Manager gestartet[1] hat, fängt W-SAM Anforderungen von Clientanwendungen an Server im internen Netzwerk und Anforderungen von auf dem Client ausgeführten Prozessen an interne Hosts ab. Sie legen diese Ressourcen auf der Registerkarte **Applications** fest, indem Sie zwei Listen konfigurieren:

- Liste **W-SAMsupported applications**

  Diese Liste enthält Anwendungen, für die W-SAM den Client/Server-verkehr zwischen dem Client und dem IVE sichern soll.

- Liste **W-SAM allowed servers**

  Diese Liste enthält Hosts, für die W-SAM den Client/Serververkehr zwischen dem Client und dem IVE sichern soll.

Wichtig: Wenn Sie anhand von W-SAM mit NetBIOS auf eine Freigabe zugreifen möchten, müssen Sie den NetBIOS-Namen des Servers (alphanumerische Zeichenfolge mit bis zu 15 Zeichen) an zwei Stellen explizit angeben: auf der Seite **Add Server** und in einer SAM-Ressourcenrichtlinie. (Platzhalter werden gegenwärtig nicht unterstützt.) Sie können auch auf der Registerkarte **SAM > Options** die Option **Auto-allow application servers** aktivieren, sodass das IVE automatisch eine SAM-Ressourcenrichtlinie erstellt, die den Zugriff auf diesen Server erlaubt.

So geben Sie Anwendungen und Server an, die mit W-SAM gesichert werden sollen:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> SAM > Applications** aus.
2. Geben Sie Ressourcen aus der Liste **W-SAM supported application** an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:
   1. Klicken Sie auf **Add Application**.

1. Sie können Secure Application Manager so konfigurieren, dass er bei der Anmeldung eines Benutzers automatisch gestartet wird. Benutzer können diese Einstellung über das Menü IVE **System > Preferences** außer Kraft setzen. Wenn der automatische Start deaktiviert ist, muss Secure Application Manager manuell gestartet werden, indem auf die entsprechende Verknüpfung im IVE-Startseitenmenü geklickt wird.

2 Geben Sie den Namen der Anwendung und bei Bedarf eine Beschreibung ein. Diese Informationen werden auf der Seite „Client Applications" für IVE-Benutzer angezeigt.

3 Wählen Sie eine der folgenden Optionen aus:

- **Standard application** – Auswahl von Citrix NFuse, Lotus Notes oder Microsoft Outlook/Exchange.
- **Custom application** – Angabe einer benutzerdefinierten Client/Server-Anwendung. Geben Sie im Feld **Filename** den Namen der ausführbaren Datei für die Datei an. Sie können darüber hinaus den Dateipfad und den MD5-Hash der ausführbaren Datei angeben. (Optional.)

  Wenn Sie einen MD5-Hash-Wert eingeben, überprüft W-SAM, ob der Prüfsummenwert der ausführbaren Datei diesem Wert entspricht. Wenn die Werte nicht übereinstimmen, teilt W-SAM dem Benutzer mit, dass die Identität der Anwendung nicht sichergestellt werden konnte, und leitet Verbindungen von der Anwendung zum IVE nicht weiter.

4 Klicken Sie auf **Save Changes** oder **Save + New**.

3. Geben Sie Ressourcen aus der Liste **W-SAM allowed servers** an, für die W-SAM den Client/Server-Verkehr zwischen dem Client und dem IVE sichert:

   1 Klicken Sie auf **Add Servers**.

   2 Geben Sie den Hostnamen (die Platzhalterzeichen „*" oder „?" sind zulässig) oder ein IP/Netzmaske-Paar an. Geben Sie mehrere Ports für einen Host als separate Einträge an.

   3 Klicken Sie auf **Add**.

4. Legen Sie in einer Secure Application Manager-Ressourcenrichtlinie fest, an welche Unternehmensressourcen (basierend auf der Kombination aus IP-Adresse und Port) das IVE eine Anwendungs- oder Serveranforderung senden kann.

   Sie können auch auf der Registerkarte **SAM > Options** die Option **Auto-allow application servers** aktivieren, sodass das IVE automatisch eine SAM-Ressourcenrichtlinie erstellt, die den Zugriff auf den angegebenen Server erlaubt. Beachten Sie, dass diese Option vor der Angabe der Anwendung bzw. des Servers aktiviert werden muss, andernfalls müssen Sie eine SAM-Ressourcenrichtlinie erstellen.

☑ Angeben von Anwendungen, die mit J-SAM gesichert werden sollen

Auf der Registerkarte **SAM > Applications** können Sie Anwendungen festlegen, für die J-SAM den Datenverkehr sichert. Beachten Sie, dass die Clientanwendung eine Verbindung mit dem lokalen Computer herstellen muss, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, damit die Java-Version von Secure Application Manager fehlerfrei verwendet werden kann. Die empfohlene Vorgehensweise für das

Zuordnen von Anwendungsservern zum lokalen PC eines Benutzers besteht in der Aktivierung der automatischen Hostzuordnung, wodurch das IVE die Datei `hosts` automatisch so ändern kann, dass Anwendungsserver an den `lokalen Host` für sichere Portumleitung geleitet werden.

Wichtig: Die automatische Hostzuordnung kann auf Windows-PCs nur erfolgen, wenn die Benutzer über Administratorberechtigungen verfügen und Secure Application Manager daher die Datei `hosts` ändern kann. Wenn Benutzer nicht über Administratorberechtigungen verfügen, wird im Secure Application Manager-Fenster eine Fehlermeldung angezeigt, und die Benutzer können nicht auf Client/Server-Anwendungen zugreifen. Wenn die Sicherheitsrichtlinie das Erteilen von Administratorberechtigungen an Benutzer nicht zulässt, können Sie die externen DNS-Server auch wie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 310 beschrieben konfigurieren.

Wenn J-SAM auf einen Clientcomputer heruntergeladen wird, enthält dieser Informationen, die Sie für die Rolle auf der Registerkarte **SAM > Applications** konfiguriert haben. Wenn ein Benutzer auf **Client Applications** klickt, wird J-SAM ausgeführt, fängt die Anforderungen an den festgelegten Ports ab und leitet sie über Ports an das IVE weiter. Das IVE leitet die Daten dann an den für den Anwendungsserver festgelegten Port weiter.

Hinweis

- Gegenwärtig wird auf Windows-, Linux- oder Macintosh-Plattformen Sun JVM, Version 1.4.1 oder höher unterstützt. Die MS JVM, die auf Sun JRE, Version 1.1 beruht, wird unter Windows ebenfalls unterstützt.
- Wenn Sie die Laufwerkzuordnung zu einem Server aktivieren möchten, müssen Sie Port 139 als Clientport und als Serverport für den betreffenden Server festlegen.

  Für Windows XP-Benutzer wird von die Registrierung vom J-SAM automatisch geändert, um Port 445 zu deaktivieren, wodurch Windows XP zur Verwendung von Port 139 bei der Laufwerkzuordnung gezwungen wird. Benutzer von Windows XP müssen einen einmaligen Neustart ausführen, damit die Änderung an der Registrierung wirksam wird. Um die von J-SAM vorgenommene Registrierungsänderung zu deaktivieren, können Benutzer auf die Schaltfläche **Restore System Settings** auf der Seite IVE **Advanced Preferences** klicken. Wenn die Änderung wieder aktiviert werden soll, müssen sie einen Neustart ausführen.

So geben Sie Anwendungen an, die mit J-SAM gesichert werden sollen:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> SAM > Applications** aus.
2. Geben Sie den Namen der Anwendung und bei Bedarf eine Beschreibung ein. Diese Informationen werden auf der Seite **Client Applications** für IVE-Benutzer angezeigt.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Standard application** – Auswahl von Citrix NFuse, Lotus Notes oder Microsoft Outlook/Exchange.
   - **Benutzerdefinierte Anwendung –**
     1 Geben Sie im Feld **Server** den DNS-Namen oder die IP-Adresse des Servers ein.
     2 Geben Sie im Feld **Server Port** den Port ein, an dem der Remoteserver die Clientverbindungen überwacht.

     Wenn beispielsweise Telnet-Verkehr von einem Remotecomputer weitergeleitet werden soll, legen Sie sowohl für den Clientport (an dem J-SAM überwacht) als auch für den Serverport (an dem der Telnet-Server überwacht) Port 23 fest.

     Hinweis: Sie aktivieren die Laufwerkzuordnung zu dieser Ressource, indem Sie 139 als Serverport eingeben.

     3 Geben Sie im Feld **Local Port** den Port ein, den J-SAM auf Verbindungen mit Clientanwendungen überwachen soll.

     Normalerweise stimmt der Wert für den lokalen Port mit dem für den Serverport überein, er unterscheidet sich in der Regel nur für Linux- oder Macintosh-Benutzer, die Anwendungen für die Portweiterleitung hinzufügen möchten, die Ports unter 1024 verwenden.

     Hinweis: Sie aktivieren die Laufwerkzuordnung zu dieser Ressource, indem Sie 139 als Serverport eingeben.

     Sie können mehrere Anwendungen an einem einzigen Port konfigurieren, beispielsweise `anw1.eigenefirma.com`, `anw2.eigenefirma.com`, `anw3.eigenefirma.com`. Das IVE weist jeder Anwendung eine Loopback-Adresse (`127.0.1.10`, `127.0.1.11`, `127.0.1.12`) zu. J-SAM überwacht diese Loopback-Adressen dann an dem festgelegten Port. Wenn beispielsweise Datenverkehr für die Adresse `127.0.1.12` am angegebenen Port vorhanden ist, leitet das IVE den Datenverkehr an den Zielhost `anw3.eigenefirma.com` weiter.

     4 Aktivieren Sie das Kontrollkästchen **Allow Secure Application Manager to dynamically select an available port ...**, wenn J-SAM den gleichen Port auf mehrere Hosts überwacht und einen verfügbaren Port

auswählen soll, falls der von Ihnen angegebene Clientport belegt ist. Um diese Option verwenden zu können, muss es die Clientanwendung ermöglichen, die Portnummer für die Verbindung festzulegen.

4. Klicken Sie auf **Save Changes** oder **Save + New**.
5. Wählen Sie unter **Enable Automatic Host Mapping (Java Version Only)** die Option **Enabled** aus, und klicken Sie dann auf **Save Changes**, wenn es sich bei den Benutzern um PC-Benutzer handelt.

   Clientanwendungen müssen Anwendungsserver zur IP-Adresse eines `localhost` auflösen. Wenn Sie die automatische Hostzuordnung für Benutzer von Remote-PCs nicht aktivieren möchten oder wenn es sich bei Ihren Benutzern um Linux-Benutzer handelt, müssen Sie Ihren externen DNS-Server zum Auflösen von Anwendungsservernamen zum `localhost` eines Benutzers konfigurieren. Detaillierte Informationen finden Sie unter „Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)“ auf Seite 310.
6. Wenn der PC eines Remotebenutzers für die Verwendung eines Webproxys in Internet Explorer eingerichtet ist, konfigurieren Sie den Clientcomputer so, dass der Proxyserver umgangen wird, wenn der Benutzer Anwendungen startet, die eine Verbindung mit Secure Application Manager herstellen müssen. Weitere Informationen finden Sie unter „Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt“ auf Seite 311.
7. Fügen Sie dem IVE DNS-Domänen hinzu, wenn Sie über mehrere interne Domänen verfügen (zum Beispiel `firma-a.com` und `firma-b.com`), sodass Namen wie zum Beispiel `anw1.firma-a.com` und `anw2.firma-b.com` ordnungsgemäß aufgelöst werden:
   1. Klicken Sie auf das Menü **Network > Network Settings**.
   2. Fügen Sie unter **DNS Name Resolution** im Feld **DNS Domains** eine durch Kommas getrennte Liste der Domänen hinzu.
   3. Klicken Sie auf **Save Changes**.

Zusätzliche Aufgaben für J-SAM

In diesem Abschnitt werden Aufgaben beschrieben, die Sie je nach den für J-SAM konfigurierten Client-/Serveranwendungen und dem von Ihren Benutzern verwendeten Betriebssystem möglicherweise durchführen müssen. Weiterhin enthält der Abschnitt Anweisungen zum Testen von J-SAM in Ihrem Unternehmen.

Folgende Themen werden behandelt:

- Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich) (310)
- Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt (311)

☑ Konfigurieren der externen DNS-Server und Benutzercomputer (falls erforderlich)

Clientanwendungen müssen Hostnamen von Servern zu J-SAM auflösen, wodurch Daten zwischen einem Client und einem Server über einen Proxy gesendet werden. Auf Windows-PCs werden Hostnamen von Servern in der Datei `hosts` gespeichert. Damit Daten mit J-SAM abgefangen werden können, müssen die Servernamen in dieser Datei zur Adresse des lokalen Computers (`localhost`) aufgelöst werden, sodass das IVE den Datenverkehr vermitteln kann. Bei der Zuordnung von Anwendungsservern zum lokalen PC eines Benutzers empfiehlt es sich, die automatische Hostzuordnung zu aktivieren (siehe (Seite 314)). Hierdurch erhält das IVE die Möglichkeit, die Datei `hosts` des PCs so zu ändern, dass Anwendungsserver auf den `localhost` des PCs verweisen, um eine sichere Portweiterleitung zu gewährleisten.

Das IVE kann nur automatische Hostzuweisung durchführen, wenn der PC-Benutzer auf dem Computer über Administratorrechte verfügt. Andernfalls müssen Sie sicherstellen, dass die internen Anwendungsservernamen extern zum `localhost` eines PCs aufgelöst werden. Fügen Sie dem externen, mit dem Internet verbundenen DNS-Server hierfür entsprechende Einträge hinzu (siehe folgende Beispiele):

```
127.0.0.1 anw1.firma-a.com
127.0.0.1 anw2.firma-b.com
127.0.0.1 exchange1.firma-a.com
127.0.0.1 exchange1.fima-b.com
```

Wenn die Clientanwendung einen unvollständigen Namen für den Anwendungsserver verwendet, müssen Benutzer DNS-Suffixe angeben, damit der PC das Suffix hinzufügen und für die Namensauflösung eine Verbindung mit dem externen DNS-Server herstellen kann. Ein Beispiel: Ein MS Outlook-Client hat üblicherweise einen unvollständigen Namen für einen MS Exchange-Server. Damit der unvollständige Name in die Adresse 127.0.0.1 aufgelöst werden kann, müssen Benutzer die entsprechenden DNS-Suffixe auf ihren PCs angeben. Das Hinzufügen von Domänennamen wirkt sich nicht auf andere Vorgänge auf dem PC aus, einschließlich der Verwendung der Clientanwendung innerhalb des Unternehmens.

So konfigurieren Sie einen Benutzer-PC mit DNS-Suffixen (Windows 2000):

1. Wählen Sie im **Startmenü** von Windows **Einstellungen > Netzwerk- und DFÜ-Verbindungen** > **LAN-Verbindung** und dann **Eigenschaften** aus.
2. Wählen Sie **Internetprotokoll (TCP/IP)** aus, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **DNS**.
4. Klicken Sie auf **Diese DNS-Suffixe anhängen** und dann auf **Hinzufügen**.
5. Fügen Sie die internen Domänen Ihres Unternehmens als zusätzliche DNS-Suffixe hinzu.

☑ Konfigurieren eines PCs, der die Verbindung mit dem IVE über einen Proxywebserver herstellt

Dieses Verfahren kann jedoch nur angewendet werden, wenn der PC eines Remotebenutzers so konfiguriert ist, dass in Internet Explorer ein Webproxy verwendet wird. Dieses Verfahren gewährleistet, dass Clientanwendungen eine Verbindung mit Secure Application Manager herstellen, statt zu versuchen, eine Verbindung mit dem Webproxy herzustellen.

So konfigurieren Sie einen PC, der in Internet Explorer eine Verbindung mit dem IVE über einen Webproxy herstellt:

1. Wählen Sie in Internet Explorer im Menü **Extras** die Option **Internetoptionen** aus.
2. Klicken Sie auf der Registerkarte **Verbindungen** auf die Schaltfläche **LAN-Einstellungen**.
3. Klicken Sie unter **Proxyserver** auf die Schaltfläche **Erweitert**.
4. Geben Sie unter „Ausnahmen" die Adressen ein, für die kein Proxyserver verwendet werden soll. Geben Sie alle Adressen (Hostnamen und `localhost`) ein, die die Clientanwendung beim Herstellen einer Verbindung über Secure Application Manager verwendet.

   Beispiele:

   Wenn der Anwendungsserver den Namen `anw1.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

   ```
   anw1;anw1.firma.com;127.0.0.1
   ```

   Wenn der Exchange-Server den Namen `exchange.firma.com` hat, geben Sie die folgenden Ausnahmen ein:

   ```
   exchange;exchange.firma.com;127.0.0.1
   ```

Registerkarte „SAM > Options“

Auf der Registerkarte **SAM > Options** können Sie allgemeine Optionen für Secure Application Manager angeben, z.B. für Start, Aktualisierung und Deinstallation von Secure Application Manager sowie zuvor bereitgestellte Ressourcen in Secure Application Manager-Ressourcenrichtlinien.

☑ Angeben allgemeiner Optionen für Secure Application Manager

So legen geben Sie allgemeine Optionen für Secure Application Manager an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> SAM > Options** aus.
2. Legen Sie unter **Secure Application Manager** die Optionen fest, die für Benutzer aktiviert werden sollen:
   - **Auto-launch Secure Application Manager** – Wenn diese Option aktiviert ist, startet das IVE Secure Application Manager automatisch, wenn sich ein Benutzer anmeldet. Wenn die Option nicht aktiviert wird, müssen Benutzer Secure Application Manager im Menü **Client Applications** manuell starten.
   - **Auto-uninstall Secure Application Manager** – Wenn diese Option aktiviert ist, deinstalliert das IVE Secure Application Manager automatisch nach der Abmeldung des Benutzers.
   - **Auto-allow application servers** – Wenn diese Option aktiviert ist, erstellt das IVE automatisch eine SAM-Ressource, die den Zugriff auf den in der Liste für W-SAM-Anwendungen und -Server sowie in der Liste der J-SAM-Anwendungen angegebenen Server zulässt.
3. Aktivieren Sie unter **Windows SAM Options** die Option **Auto-upgrade Secure Application Manager**, damit das IVE Secure Application Manager bei einer Benutzeranmeldung automatisch aktualisiert.
4. Legen Sie unter **Java SAM Options** die Optionen fest, die für Benutzer aktiviert werden sollen:
   - **User can add applications** – Diese Option ermöglicht Benutzern das Hinzufügen von Anwendungen. Damit Benutzer Anwendungen hinzufügen können, müssen Sie den DNS-Namen und die Client/Serverports des Anwendungsservers kennen.

     Wenn Sie diese Option aktivieren, können Benutzer die Portumleitung zu einem beliebigen Host oder Port im Unternehmen einrichten. Bevor Sie Benutzern die Möglichkeit geben, Anwendungen hinzuzufügen, vergewissern Sie sich, dass diese Funktion mit Ihren Sicherheitsanfor-

derungen vereinbar ist. Wenn ein Benutzer eine Anwendung hinzufügt, bleibt diese für den Benutzer auch dann verfügbar, wenn die Funktion später deaktiviert wird.

- **Automatic host-mapping** – Diese Option ermöglicht es Secure Application Manager, die Datei „hosts" des Windows-PCs zu bearbeiten und Einträge von Windows-Anwendungsservern durch localhost zu ersetzen. Diese Einträge werden auf die Originaldaten zurückgesetzt, wenn ein Benutzer Secure Application Manager schließt.

  Die Java-Version von Secure Application Manager kann nur dann verwendet werden, wenn zwischen der Clientanwendung und dem lokalen PC, auf dem Secure Application Manager als Anwendungsserver ausgeführt wird, eine Verbindung eingerichtet wird. Bei der Zuordnung von Anwendungsservern zum lokalen PC eines Benutzers empfiehlt es sich, die automatische Hostzuordnung zu aktivieren. Das IVE kann dann die Datei „hosts" automatisch so ändern, dass Anwendungsserver für sichere Portumleitung zum lokalen Host des PCs geleitet werden. Sie können auch den externen DNS-Server konfigurieren.

- **Skip web-proxy registry check** – Wenn diese Option aktiviert ist, überprüft J-SAM die Registrierung des Benutzers nicht auf einen Webproxy. Manche Benutzer sind nicht berechtigt, die eigene Registrierung einzusehen. Wenn J-SAM versucht, die Registrierung aufzurufen, kann dem Benutzer daher ein Fehler aufgrund fehlender Berechtigungen angezeigt werden. Die Auswahl dieser Option gewährleistet, dass Benutzern diese Meldung nicht angezeigt wird.

5. Klicken Sie auf **Save Changes**.

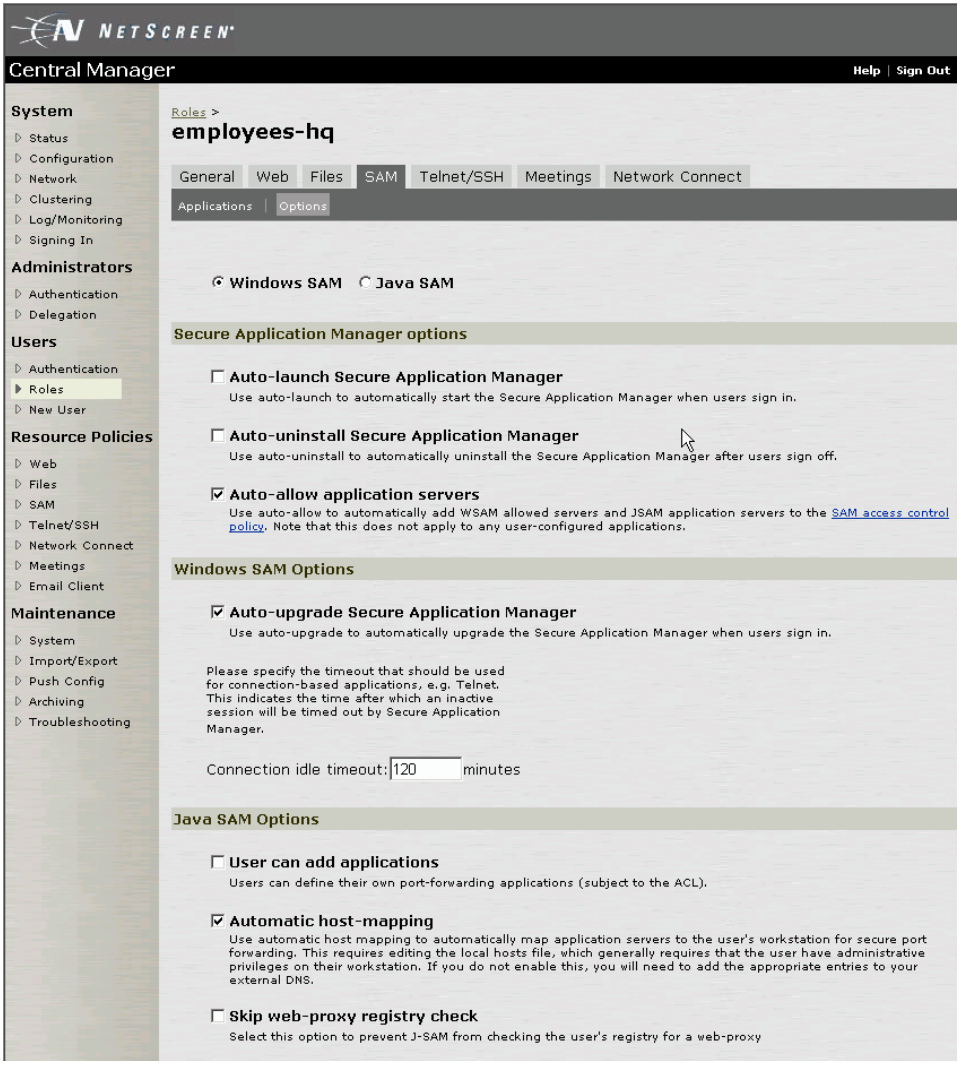

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
employees-hq
General
Web
Files
SAM
Telnet/SSH
Meetings
Network Connect
Applications
Options
Windows SAM
Java SAM
Secure Application Manager options
Auto-launch Secure Application Manager
Use auto-launch to automatically start the Secure Application Manager when users sign in.
Auto-uninstall Secure Application Manager
Use auto-uninstall to automatically uninstall the Secure Application Manager after users sign off.
Auto-allow application servers
Use auto-allow to automatically add WSAM allowed servers and JSAM application servers to the SAM access control policy. Note that this does not apply to any user-configured applications.
Windows SAM Options
Auto-upgrade Secure Application Manager
Use auto-upgrade to automatically upgrade the Secure Application Manager when users sign in.
Please specify the timeout that should be used for connection-based applications, e.g. Telnet. This indicates the time after which an inactive session will be timed out by Secure Application Manager.
Connection idle timeout: 120 minutes
Java SAM Options
User can add applications
Users can define their own port-forwarding applications (subject to the ACL).
Automatic host-mapping
Use automatic host mapping to automatically map application servers to the user's workstation for secure port forwarding. This requires editing the local hosts file, which generally requires that the user have administrative privileges on their workstation. If you do not enable this, you will need to add the appropriate entries to your external DNS.
Skip web-proxy registry check
Select this option to prevent J-SAM from checking the user's registry for a web-proxy

Abbildung 90: Users > Roles > *Ausgewählte Rolle* > SAM >Options

Registerkarte „Telnet/SSH > Sessions“

Auf der Registerkarte **Telnet/SSH > Sessions** können Sie Lesezeichen für sichere Terminalsitzungen erstellen, die dieser Rolle zugeordneten Benutzern auf der Willkommensseite angezeigt werden. In Lesezeichen für Terminalsitzungen sind Informationen zu Terminalsitzungen für Telnet- oder SSH-Sitzungen festgelegt, die von Benutzer gestartet werden können Diese Sitzungen gewähren Benutzern Zugriff auf eine Reihe von vernetzten Geräten, beispielsweise UNIX-Server, Netzwerkgeräte und Legacyanwendungen, die das Terminal verwenden.

Wenn Sie die Aktualisierungsoption Secure Terminal Access aktivieren (Telnet/SSH), den Benutzern jedoch nicht die Möglichkeit bieten, eigene Lesezeichen zu erstellen, müssen Sie unbedingt die Sitzungslesezeichen für sie konfigurieren. Andernfalls können Benutzer diese Funktion nicht nutzen.

Hinweis: Gegenwärtig wird die Sun JVM in der Version 1.4.1 oder höher unterstützt.

☑ Erstellen von Lesezeichen für sichere Terminalsitzungen

So erstellen Sie Lesezeichen für sichere Terminalsitzungen:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Telnet/SSH > Sessions** aus.
2. Klicken Sie auf **Add Session**, und geben Sie die erforderlichen Informationen ein, die durch ein Sternchen (*) gekennzeichnet sind. Wenn Sie einen Namen und eine Beschreibung für ein Lesezeichen angeben, werden diese Informationen auf der Seite **Terminal Sessions** angezeigt.
3. Klicken Sie auf **Save Changes** oder **Save + New**.

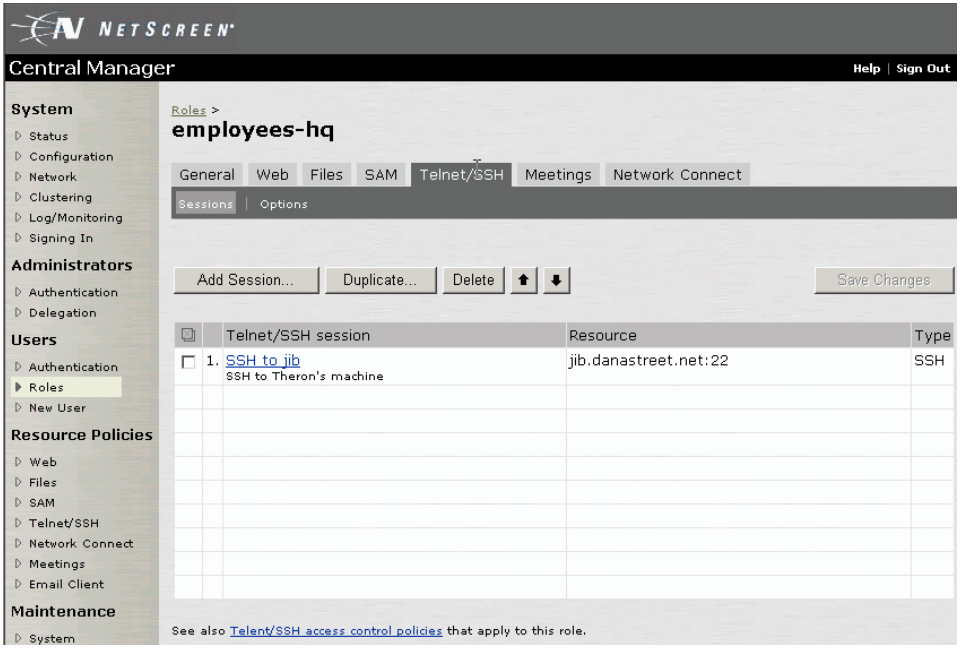


Abbildung 91: Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Sessions

Registerkarte „Telnet/SSH > Options“

Auf der Registerkarte **Telnet/SSH > Options** können Sie allgemeine Optionen für Telnet/SSH festlegen. Diese Optionen werden zusammen mit den Telnet/SSH-Ressourcenrichtlinien verwendet.

☑ Angeben allgemeiner Optionen für Telnet/SSH

So geben Sie allgemeine Optionen für Telnet/SSH an:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Telnet/SSH > Options** aus.
2. Aktivieren Sie **User can add sessions**, um Benutzer zu erlauben, eigene Sitzungslesezeichen zu definieren. Wenn Sie diese Option aktivieren, wird auf der Seite **Terminal Sessions** die Schaltfläche **Add Terminal Session** angezeigt, wenn ein Benutzer die IVE-Willkommensseite das nächste Mal aktualisiert.

3. Aktivieren Sie **Auto-allow role Telnet/SSH sessions**, um dem IVE die automatische Erstellung einer Telnet/SSH-Ressourcenrichtlinie zu ermöglichen, die den Zugriff auf den im Sitzungslesezeichen angegebenen Server zulässt.
4. Klicken Sie auf **Save Changes**.

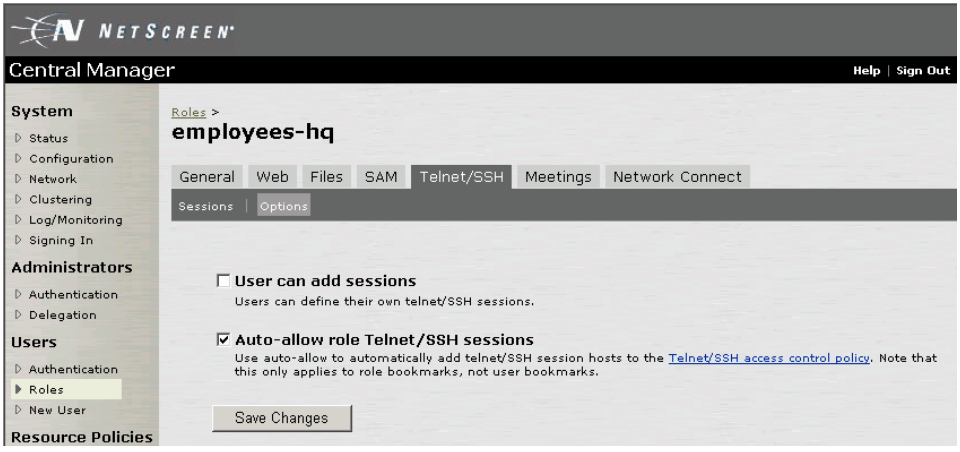


Abbildung 92: Users > Roles > *Ausgewählte Rolle* > Telnet/SSH > Options

Registerkarte „Meetings“

Auf der Registerkarte **Meetings** können Sie zu einem beliebigen Zeitpunkt festlegen, welche Benutzerrollen Konferenzen planen können (siehe unter „Secure Meeting – Übersicht“ auf Seite 13), um die Sicherheitsstufen für die zu erstellenden Konferenzen zu steuern und um die für Konferenzen verwendeten Systemressourcen zu verwalten.

Beachten Sie bei der Erstellung von Benutzerrollen Folgendes: Wenn Benutzer mehreren Rollen zugeordnet sind und Sie diese zusammenführen (Seite 277), werden alle Optionen auf der Seite **User > Roles > Meetings** mit Ausnahme der Richtlinieneinstellungen zusammengeführt, sodass Sie erweiterten Zugriff gewähren, der jedoch zu Lasten der Sicherheit geht. Wenn die Richtlinieneinstellungen angewendet werden, die die Anzahl der Konferenzen und der pro Rolle zulässigen Teilnehmer steuern, durchläuft Secure Meeting die verschiedenen Rollen, um solche zu finden, deren Höchstzahl noch nicht erreicht ist.

Sie können z.B. festlegen, dass die folgenden Rollen die angegebene Anzahl von Konferenzen planen können:

- Entwicklung: 25 Konferenzen
- Management: 50 Konferenzen
- Vertrieb: 200 Konferenzen

Wenn Joe diesen Rollen (in der genannten Reihenfolge) zugeordnet ist und versucht, eine Konferenz zu planen, überprüft Secure Meeting zunächst, ob die zulässige Anzahl geplanter Konferenzen für die Rolle „Entwicklung" bereits erreicht ist. Wenn dies der Fall ist, überprüft Secure Meeting die Konferenzanzahl für die Rolle „Management". Wenn auch hier die Höchstzahl erreicht ist, überprüft Secure Meeting diejenige für die Rolle „Vertrieb". Nur wenn die Höchstzahl für alle Rollen erreicht ist, wird Joe von Secure Meeting eine Meldung angezeigt, dass die Höchstzahl geplanter Konferenzen erreicht ist und er keine Konferenz erstellen kann. Die Anzahl von Konferenzen oder Konferenzteilnehmern kann nicht auf Bereichsebene begrenzt werden.

☑ Aktivieren und Konfigurieren von Konferenzen für Benutzerrollen

So aktivieren und konfigurieren Sie Konferenzen:

1. Wählen Sie in der Web console **Users > Roles** aus.
2. Wählen Sie eine Rolle aus.
3. Aktivieren Sie auf der Registerkarte **General > Overview** das Kontrollkästchen **Meetings**, und klicken Sie auf **Save Changes**.

Wichtig: Wenn Sie das Kontrollkästchen **Meetings** nicht aktivieren, können Benutzer Konferenzen weder erstellen noch planen und den Secure Meeting-Kalender nicht anzeigen. Sie können jedoch trotzdem an den Konferenzen teilnehmen, zu denen sie eingeladen sind. Dazu klicken sie auf die Verknüpfung in der E-Mail mit der Einladung, oder sie geben den Konferenz-URL direkt in den Webbrowser ein.

---

4. Klicken Sie auf die Registerkarte **Meetings**.
5. Geben Sie im Bereich **Meeting Options** die Zugriffsebene an, die Benutzern gewährt werden soll:
   - **Allow user to join meetings**. Bei Auswahl dieser Option können Konferenzen nicht erstellt oder geplant werden, Benutzer können jedoch auf den Secure Meeting-Kalender zugreifen, um den Konferenzen beizutreten, zu denen sie eingeladen sind.
   - **Allow user to create and join meetings**. Bei Auswahl dieser Option können Benutzer mithilfe des Secure Meeting-Kalenders

(zugänglich über die Verknüpfung **Meetings** auf der Startseite des Endbenutzers) Konferenzen erstellen, planen und auf diese zugreifen.

6. Geben Sie die **Authentication Requirements** an, die Benutzer auf von ihnen erstellte Konferenzen anwenden sollen:
   - **Meeting password optional (more accessible)**. Bei Auswahl dieser Option wird dem Ersteller der Konferenz die Entscheidung darüber überlassen, ob für die Teilnahme an der Konferenz ein Kennwort erforderlich ist. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort (sofern vorhanden) kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require meeting password (more secure)**. Bei Auswahl dieser Option muss der Ersteller der Konferenz entweder ein Kennwort für die Konferenz erstellen oder das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require server-generated password (even more secure)** Bei Auswahl dieser Option muss der Ersteller der Konferenz das von Secure Meeting erzeugte Kennwort verwenden. Wenn Sie diese Option auswählen, kann jeder, der den URL, die ID-Nummer und das Kennwort kennt, an der Konferenz teilnehmen, nicht nur IVE-Benutzer.
   - **Require secure gateway authentication (most secure)**. Bei Auswahl dieser Option können nur solche eingeladene Benutzer an Konferenzen teilnehmen, die am sicheren IVE-Gateway authentifiziert wurden. Wenn Sie diese Option auswählen, muss der Ersteller der Konferenz kein Kennwort für die Konferenz erstellen, da sich alle Benutzer am sicheren IVE-Gateway authentifizieren müssen.
7. Geben Sie die Methode für **Password Distribution** an, die von den Erstellern von Konferenzen angewendet werden soll:
   - **Do not display the password in the notification email (more secure)**. Bei Auswahl dieser Option müssen Ersteller von Konferenzen das Konferenzkennwort manuell an die eingeladenen Teilnehmer verteilen (und nicht automatisch über die von Secure Meeting versendeten E-Mail-Benachrichtigungen). Wenn das Kennwort nicht in der Konferenz-E-Mail enthalten ist, erhöht dies die Sicherheit für die Konferenz.
   - **Display the password in the notification email (more accessible)**. Bei Auswahl dieser Option wird das Konferenzkennwort automatisch über die E-Mail-Benachrichtigung verteilt, die von Secure Meeting gesendet wird.
   - **Allow the meeting creator to decide**. Bei Auswahl dieser Option kann der Ersteller der Konferenz festlegen, ob das Konferenzkennwort

über die automatisch von Secure Meeting versendeten E-Mail-Benachrichtigungen verteilt werden soll.

8. Geben Sie an, ob Sie Vorführenden der Konferenz ermöglichen möchten, die Steuerung ihrer Desktops und Anwendungen mit anderen Teilnehmern der Konferenz zu teilen, indem Sie im Bereich **Remote Control** eine der folgenden Optionen auswählen:
   - **Allow remote control of shared windows (more functional).** Die Auswahl dieser Option erlaubt dem Vorführenden oder Leiter der Konferenz, die Steuerung des Desktops und der Desktopanwendungen des Vorführenden an einen beliebigen Teilnehmer der Konferenz abzugeben, nicht nur an IVE-Benutzer.
   - **Disable remote control (more secure).** Die Auswahl dieser Option beschränkt die Steuerung des Desktops und der Desktopanwendungen des Vorführenden der Konferenz ausschließlich auf den Vorführenden selbst.
9. Geben Sie im Bereich **Meeting Policy Settings** an, ob Sie die von Secure Meeting-Benutzern verwendeten Ressourcen einschränken möchten:
   - Aktivieren Sie das Kontrollkästchen **Limit number of scheduled meetings**, und geben Sie einen entsprechenden Wert für die Höchstanzahl von Konferenzen ein, die zu einem bestimmten Zeitpunkt für die Rolle geplant werden kann.
   - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meetings**, und geben Sie einen entsprechenden Wert für die Höchstanzahl von Konferenzen ein, die gleichzeitig von Mitgliedern der Rolle abgehalten werden kann.
   - Aktivieren Sie das Kontrollkästchen **Limit number of simultaneous meeting attendees**, und geben Sie einen entsprechenden Wert für die Höchstanzahl von Personen ein, die gleichzeitig an von Mitgliedern der Rolle geplanten Konferenzen teilnehmen können.
   - Aktivieren Sie das Kontrollkästchen **Limit duration of meetings (minutes)**, und geben Sie einen entsprechenden Wert (in Minuten) für die maximale Dauer einer Konferenz ein.

Wichtig: Das IVE begrenzt die Anzahl von Konferenzen, an denen Benutzer teilnehmen können. Ein einzelner Benutzer kann pro Computer stets nur an einer Konferenz und innerhalb von jeweils 3 Minuten an höchstens 10 aufeinanderfolgenden Konferenzen teilnehmen. Diese Begrenzungen werden zusätzlich zu den Konferenz- und Benutzerbegrenzungen angewendet, die in Ihrer Secure Meeting-Lizenz festgelegt sind.

---

10. Klicken Sie auf **Save Changes**. Das IVE fügt auf den Startseiten von sicheren Gateways für Benutzer mit der festgelegten Rolle eine Verknüpfung mit der Bezeichnung **Meeting** hinzu.

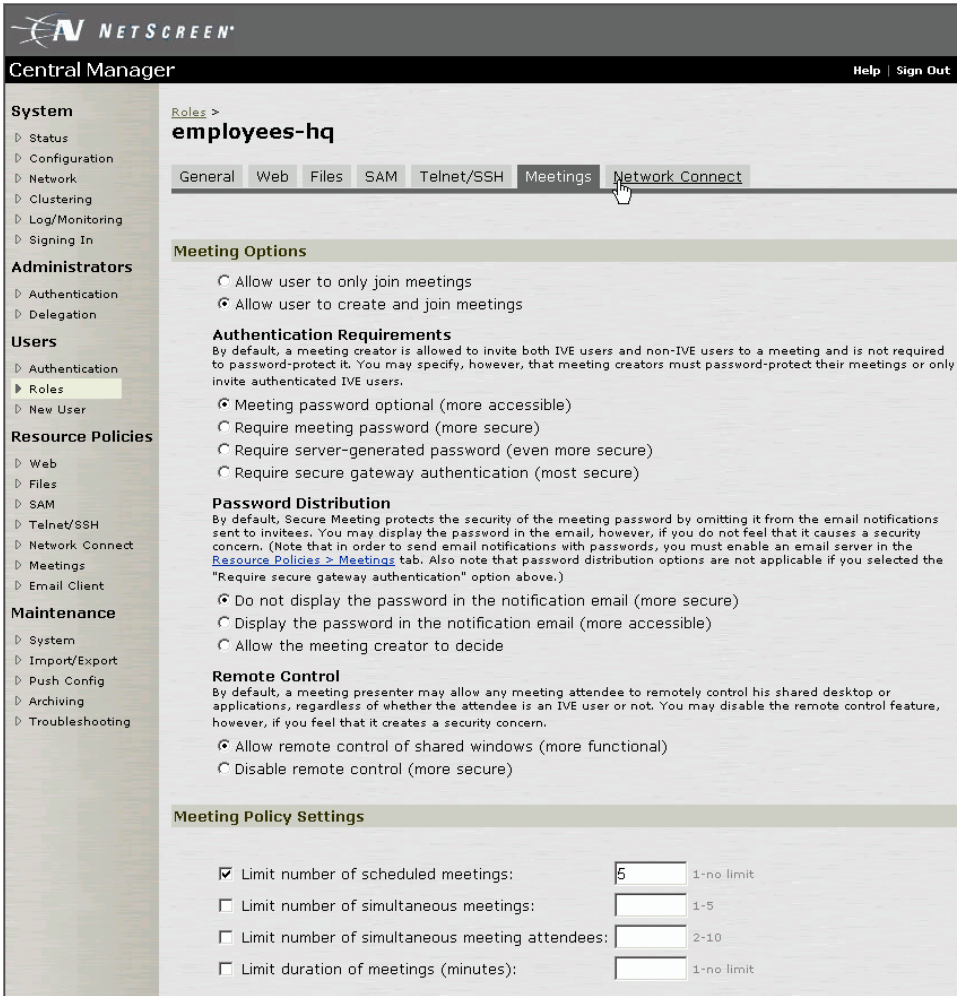

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Roles >
employees-hq
General
Web
Files
SAM
Telnet/SSH
Meetings
Network Connect
Meeting Options
Allow user to only join meetings
Allow user to create and join meetings
Authentication Requirements
By default, a meeting creator is allowed to invite both IVE users and non-IVE users to a meeting and is not required to password-protect it. You may specify, however, that meeting creators must password-protect their meetings or only invite authenticated IVE users.
Meeting password optional (more accessible)
Require meeting password (more secure)
Require server-generated password (even more secure)
Require secure gateway authentication (most secure)
Password Distribution
By default, Secure Meeting protects the security of the meeting password by omitting it from the email notifications sent to invitees. You may display the password in the email, however, if you do not feel that it causes a security concern. (Note that in order to send email notifications with passwords, you must enable an email server in the Resource Policies > Meetings tab. Also note that password distribution options are not applicable if you selected the "Require secure gateway authentication" option above.)
Do not display the password in the notification email (more secure)
Display the password in the notification email (more accessible)
Allow the meeting creator to decide
Remote Control
By default, a meeting presenter may allow any meeting attendee to remotely control his shared desktop or applications, regardless of whether the attendee is an IVE user or not. You may disable the remote control feature, however, if you feel that it creates a security concern.
Allow remote control of shared windows (more functional)
Disable remote control (more secure)
Meeting Policy Settings
Limit number of scheduled meetings:
5
1-no limit
Limit number of simultaneous meetings:
1-5
Limit number of simultaneous meeting attendees:
2-10
Limit duration of meetings (minutes):
1-no limit

Abbildung 93: Users > Roles > *Ausgewählte Rolle* > Meetings

Registerkarte „Network Connect“

Auf der Registerkarte **Network Connect** können Sie die Option für das lokale Subnetz festlegen.

☑ Festlegen der Option für das lokale Subnetz von Network Connect

So legen Sie die Option für das lokale Subnetz von Network Connect fest:

1. Wählen Sie in der Webkonsole **Users > Roles >** *Ausgewählte Rolle* **> Network Connect** aus.
2. Aktivieren Sie **Allow access to local subnet**, um in der Routingtabelle die Route des lokalen Subnetzes beizubehalten. Die Routingtabelle kann bearbeitet werden.
3. Klicken Sie auf **Save Changes**.

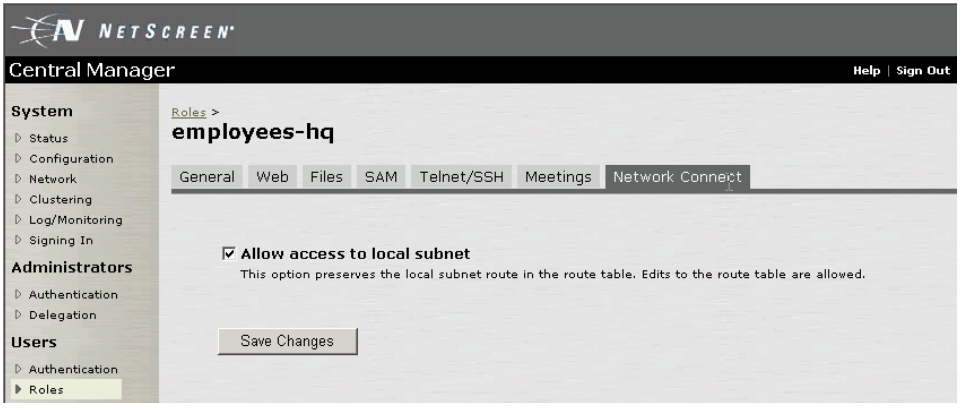


Abbildung 94: Users > Roles > *Ausgewählte Rolle* > Network Connect

Konfigurieren der Seite „New User“

☑ Erstellen **lokaler Benutzer**

Wenn Sie als Typ des Authentifizierungsservers „IVE Authentication“ auswählen, müssen Sie für diese Datenbank Datensätze für lokale Benutzer definieren. Ein Datensatz für einen lokalen Benutzer besteht aus einem Benutzernamen, dem vollständigen Namen und dem Kennwort des Benutzers. Datensätze für lokale Benutzer können für Benutzer erstellt werden, die normalerweise von einem externen Authentifizierungsserver überprüft werden, den Sie deaktivieren möchten. Dies bietet sich auch an, wenn Sie schnell eine Gruppe von temporären Benutzern erstellen möchten.

So erstellen Sie lokale Benutzerdatensätze für die lokale IVE-Authentifizierung:

1. Führen Sie in der Web console einen der folgenden Vorgänge aus:
   - Wählen Sie **System > Signing In > Servers** aus, und klicken Sie auf die IVE-Datenbank, der Sie ein Benutzerkonto hinzufügen möchten. Klicken Sie auf die Registerkarte **Users** und dann auf **New**.
   - Wählen Sie **Users > New User** aus.
2. Geben Sie den Benutzernamen, den vollständigen Namen des Benutzers und ein Kennwort ein. Hinweis:
   - In Benutzernamen darf die Zeichenkombination „~~“ nicht enthalten sein.
   - Wenn Sie den Benutzernamen eines Benutzers nach dem Erstellen seines Kontos ändern möchten, müssen Sie ein neues Konto erstellen.
3. (Nur auf der Seite **Users > New User**) Wählen Sie aus der Liste **Authenticate Using** die IVE-Datenbank aus, der Sie ein Benutzerkonto hinzufügen möchten.
4. Klicken Sie auf **Save Changes**. Der Benutzerdatensatz wird der IVE-Datenbank hinzugefügt.

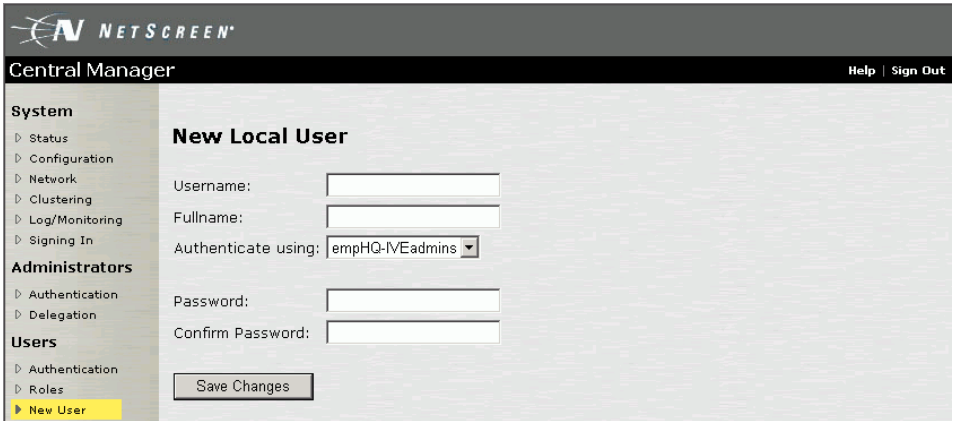


Abbildung 95: Users > New User

Konfigurieren der Seite „Web“

Die Seite **Resource Policies > Web** enthält die folgenden Registerkarten:

Registerkarte „Access“ 330
Registerkarte „Caching > Policies“ 331
Registerkarte „Caching > Options“ 335
Registerkarte „Java > Access Control“ 336
Registerkarte „Java > Code Signing“ 337
Registerkarte „Rewriting > Selective Rewriting“ 339
Registerkarte „Rewriting > Pass-through Proxy“ 340
Registerkarte „Remote SSO > Form POST“ 342
Registerkarte „Remote SSO > Headers/Cookies“ 345
Registerkarte „Web Proxy > Policies“ 346
Registerkarte „Web Proxy > Settings“ 348

Auf der Seite **Resource Policies > Web** können Sie Folgendes durchführen:

Schreiben einer Ressourcenrichtlinie für den Webzugriff 330
Schreiben einer Ressourcenrichtlinie für die Zwischenspeicherung 332
Angeben von Zwischenspeicheroptionen 335
Schreiben einer Ressourcenrichtlinie für die Java-Zugriffsteuerung 336
Schreiben einer Ressourcenrichtlinie für die Java-Codesignatur 337
Schreiben einer Ressourcenrichtlinie für selektives Neuschreiben 339
Schreiben einer Ressourcenrichtlinie für Durchgangsproxys 341
Schreiben einer Ressourcenrichtlinie für Remote-SSO Form POST 342
Schreiben einer Ressourcenrichtlinie für SSO-Header und -Cookies 345
Schreiben einer Ressourcenrichtlinie für Webproxys 346
Angeben von Einstellungen für Webproxys 348

Schreiben einer Webressourcenrichtlinie

Wenn Sie einer Rolle Zugriff auf das Web gewähren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Ressourcen ein Benutzer zugreifen darf, ob das IVE den vom Benutzer angeforderten Inhalt neu schreiben muss sowie Angaben zu Zwischenspeicherung, zum Applet und zu Anforderungen für die Einzelanmeldung machen. Für jede Webanforderung ermittelt das IVE die konfigurierten[1] Richtlinien für das

1. Wenn Sie kein Neuschreiben von Ressourcenrichtlinien („Rewriting“) konfigurieren, setzt das IVE die Auswertung anhand der Richtlinien fort, die für die Anforderung des Benutzers gelten.

Neuschreiben. Wenn der Benutzer eine Ressource anfordert, die nicht neu geschrieben werden darf („don't rewrite"), weil sie entweder selektiv neu geschrieben werden soll oder aufgrund einer Ressourcenrichtlinie für Durchgangsproxy, leitet das IVE die Anforderung des Benutzers an die entsprechende Back-End-Ressource weiter. Andernfalls setzt das IVE die Auswertung der Ressourcenrichtlinien fort, die der Anforderung entsprechen, wie z.B. Java-Ressourcenrichtlinien bei der Anforderung eines Java-Applet. Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Webressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Webrichtlinie müssen Sie Webserver oder bestimmte URLs angeben. Weitere Informationen finden Sie unter „Angeben von Webressourcen" auf Seite 46.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.
- **Aktionen:** Jeder Typ von Ressourcenrichtlinie führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion, wie Neuschreiben von Inhalten, Neusignieren von Applets, Bereitstellen von Webdaten ausführen bzw. nicht ausführen. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

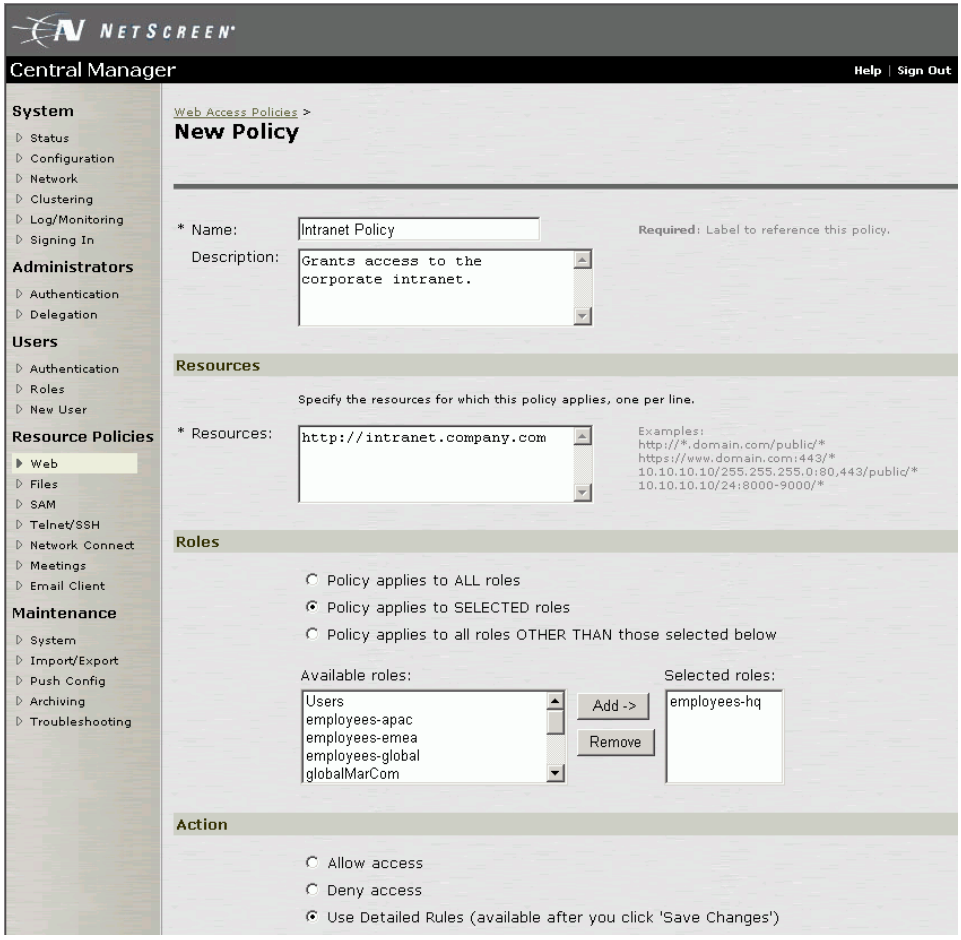


Abbildung 96: Resource Policies > Web > Access > New Policy

Diese Abbildung zeigt eine typische **New Policy**-Konfigurationsseite für eine Webressourcenrichtlinie. Weitere Informationen zum Eingeben der Informationen in die Liste **Resources** finden Sie unter „Angeben von Ressourcen für eine Ressourcenrichtlinie“ auf Seite 45.

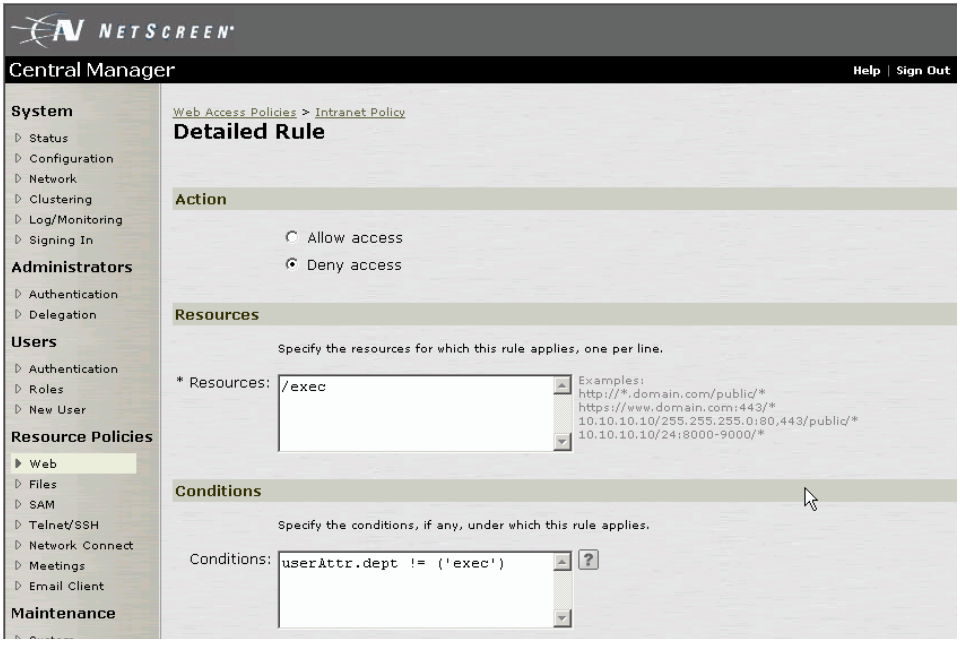


Abbildung 97: Resource Policies > Web > Access > New Policy > Detailed Rule
Diese Abbildung zeigt, wie einer Richtlinie eine detaillierte Regel hinzugefügt wird. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.

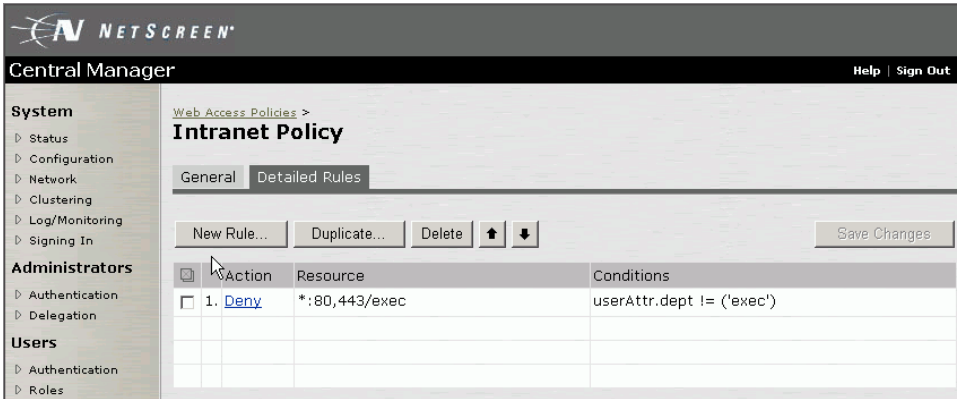


Abbildung 98: Resource Policies > Web > Access > New Policy > Detailed Rule Added
Informationen über detaillierte Regeln finden Sie auf der Registerkarte **Detailed Rules** für eine Richtlinie und auf der Hauptseite einer Ressourcenrichtlinie, indem Sie in der Spalte **Action** auf *Details* klicken (**Abbildung 99** auf Seite 329).

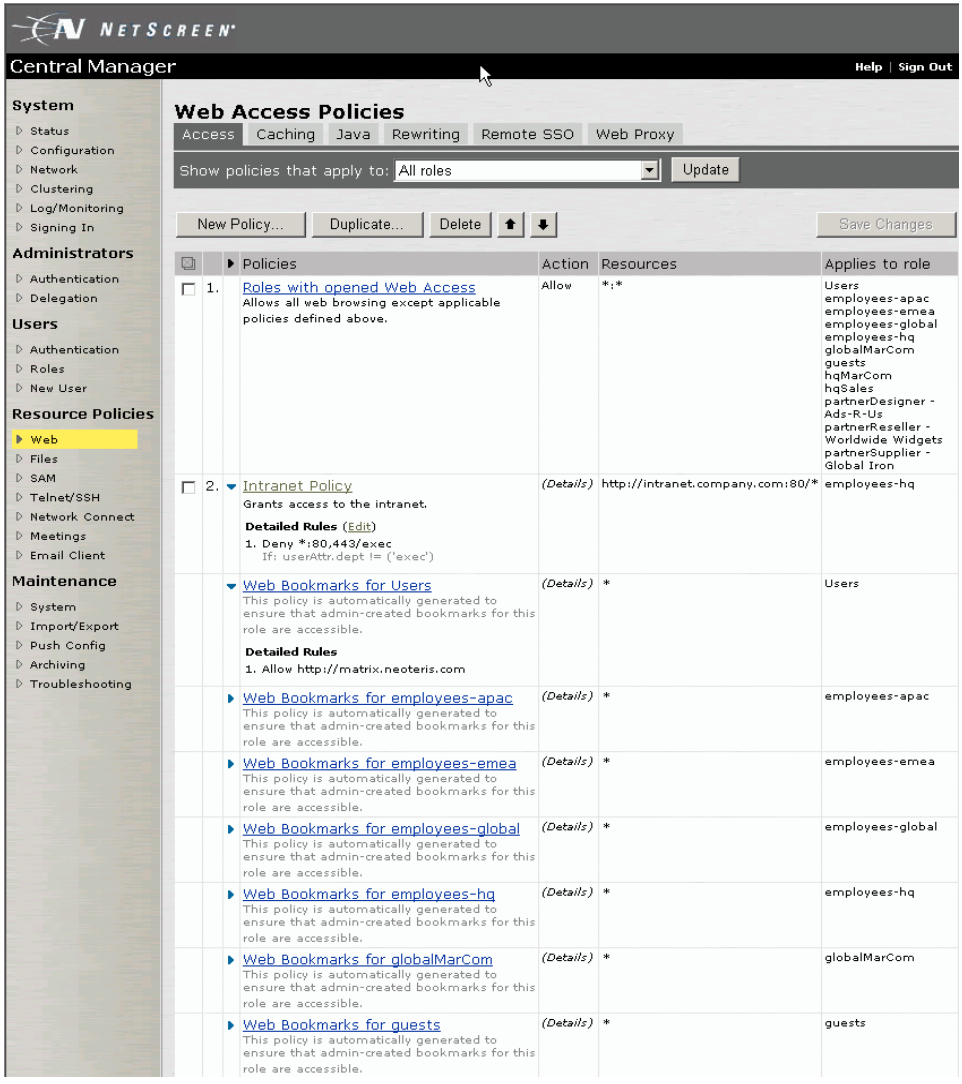


Abbildung 99: Resource Policies > Web > Access

Diese Abbildung zeigt die Seite „Policies" der Ressourcenrichtlinie für Webzugriff. Mit der auf der Registerkarte Users > Roles > Web > Option aktivierten Option für automatische Erlaubnis werden Richtlinien erstellt, die gewährleisten, dass Benutzer die für die Rolle erstellten Weblesezeichen zugreifen können.

Registerkarte „Access“

Auf der Registerkarte **Access** können Sie eine Webressourcenrichtlinie schreiben, die steuert, auf welche Webressourcen Benutzer zugreifen dürfen, um eine Verbindung mit dem Internet, Intranet oder Extranet herzustellen. Sie können den Zugriff auf Webressourcen nach URL oder IP-Bereich zulassen bzw. verweigern. Für URLs können Sie die Platzhalter „*“ und „?“ verwenden, um mehrere Hostnamen und Pfade effektiv anzugeben. Für Ressourcen, die Sie nach Hostnamen angeben, können Sie außerdem entweder HTTP, HTTPS oder beide Protokolle auswählen.

☑ Schreiben einer Ressourcenrichtlinie für den Webzugriff

So schreiben Sie eine Ressourcenrichtlinie für den Webzugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Access** aus.
2. Klicken Sie auf der Seite **Web Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Web Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Caching > Policies“

Auf der Registerkarte **Caching > Policies** können Sie eine Webressourcenrichtlinie schreiben, die steuert, welche Webinhalte auf einem Benutzercomputer zwischengespeichert werden. Die Zwischenspeicherung im Browser ist standardmäßig deaktiviert, sodass das IVE sämtliche Seiten, die für Remotebenutzer bereitgestellt werden, als nicht zwischenspeicherungsfähig markiert. Durch diese Einstellung wird verhindert, dass vertrauliche Seiten auf Remotecomputern verbleiben, nachdem ein Benutzer den Browser geschlossen hat. Diese Option kann jedoch auch zu einer Verlangsamung des Browsers führen, weil sie zum wiederholten Abrufen von Inhalten führt. Bei sehr langsamen Verbindungen können Probleme mit der Systemleistung auftreten. Alternativ können Sie eine Richtlinie angeben, die gestattet, dass einige Inhalte wie Bilder, die eine bestimmte Größenbeschränkung nicht überschreiten, zwischengespeichert werden können.

Browserunterstützung

Bei den Cachesteuerungsdirektiven handelt es sich um W3C-Standards, die von allen kompatiblen Browsern unterstützt werden. In der folgenden Liste der von IVE unterstützten Browser werden Cachesteuerungs-Header berücksichtigt:

- Win2k-IE5.5 SP2
- Win2k-IE6.0
- Win98-Netscape4.79
- Win98-IE5.5, SP2
- MacOS9.2-IE5.1.5
- MacOSx-IE5.2

☑ Schreiben einer Ressourcenrichtlinie für die Zwischenspeicherung

So schreiben Sie eine Ressourcenrichtlinie für die Webzwischenspeicherung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Policies** aus.
2. Klicken Sie auf der Seite **Web Caching Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Smart Caching** (Headers senden, die für Inhalt und Browser geeignet sind)

     Falls das IVE im "user-agent"-Header „msie" oder „windows-media-player" erkennt und sich die Anforderung auf eine Mediendatei bezieht, sendet das IVE keinen Antwortheader `cache` oder `cache-control:no-store`.

     Beispiel:

     ```
     (wenn in „content type“ das Element „audio/x-pn-realaudio“ steht
     ODER
      wenn „content type“ mit „video/“ beginnt ODER
      wenn „content type“ mit „audio/“ beginnt ODER
      wenn „content type“ gleich „application/octet-stream“ ist und
     die
       Dateierweiterung mit „rm“ oder „ram“ beginnt
     )
     ```

     In diesen Fällen entfernt das IVE den `cache-control`-Header des Ursprungsservers, und der Inhalt kann zwischengespeichert werden. Durch dieses Verhalten können Mediendateien ordnungsgemäß funktionieren.

     Wenn das IVE im Benutzer-Agent-Header „msie" oder „windows-media-player" erkennt

     - und sich die Anforderung auf Flash-Dateien, XLS-, PPS- und PPT-Dateien bezieht,
     - und der „Content-Type" application/, text/rtf, text/xml, model/ ist oder
     - wenn der Ursprungsserver einen „Content-Disposition"-Header sendet,

     sendet das IVE den `cache-control:no-store`-Header und entfernt den Cachesteuerungs-Header des Ursprungsservers.

     In allen anderen Fällen fügt das IVE die Antwortheader `pragma:no-cache` oder `cache-control:no-store` hinzu.

     Hinweis: ICA-Dateien von Citrix und QuickPlace-Dateien werden anders behandelt. ICA-Dateien von Citrix sind immer zwischenspeicherungsfähig und erhalten auch den Header „cache-control-private“. QuickPlace-Dateien, die keiner festgelegten Regel (die Vorrang hat) entsprechen, erhalten die Header CCNS und „cache-control:private“.

- **Don't Cache** („Cache Control: No-Store“ senden)

  Das IVE entfernt die Cachesteuerungs-Header des Ursprungsservers und fügt stattdessen einen Antwortheader vom Typ `cache-control:no-store` hinzu, falls die vom Browser gesendete User-Agent-Zeichenfolge „msie“ oder „windows-media-player“ enthält.

- **Don't Cache** („Pragma: No Cache“ senden)

  Das IVE fügt der Antwort Header vom Typ `pragma:no-cache` und `cache-control:no-cache` hinzu. Darüber hinaus leitet das IVE die Cacheheader des Ursprungsservers (beispielsweise `age`, `date`, `etag`, `last-modified`, `expires`) nicht weiter.

- **Cache** (Cacheheader nicht hinzufügen/ändern)

  Das IVE fügt keine Antwortheader „pragma:nocache“ oder „cachecontrol:nostore“ hinzu und leitet die Cacheheader des Ursprungsservers weiter.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Web Caching Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Caching > Options“

Auf der Registerkarte **Caching > Options** können Sie die maximale Größe einer Bilddatei angeben, die auf einem Client zwischengespeichert werden kann. Wenn der „Content-Type“-Header des Ursprungsservers mit „image/“ beginnt und der „Content-Length“-Header eine Größe unter der angibt, die in dieser Option als maximale Größe konfiguriert ist, leitet das IVE die Cacheheader des Ursprungsservers weiter. Andernfalls behandelt das IVE die Anforderung wie bei deaktivierter Zwischenspeicherung.

☑ Angeben von Zwischenspeicheroptionen

So geben Sie Zwischenspeicheroptionen an:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Caching > Options** aus.
2. Klicken Sie auf der Seite **Caching Policies** auf **New Policy**.
3. Klicken Sie auf **Save Changes**.

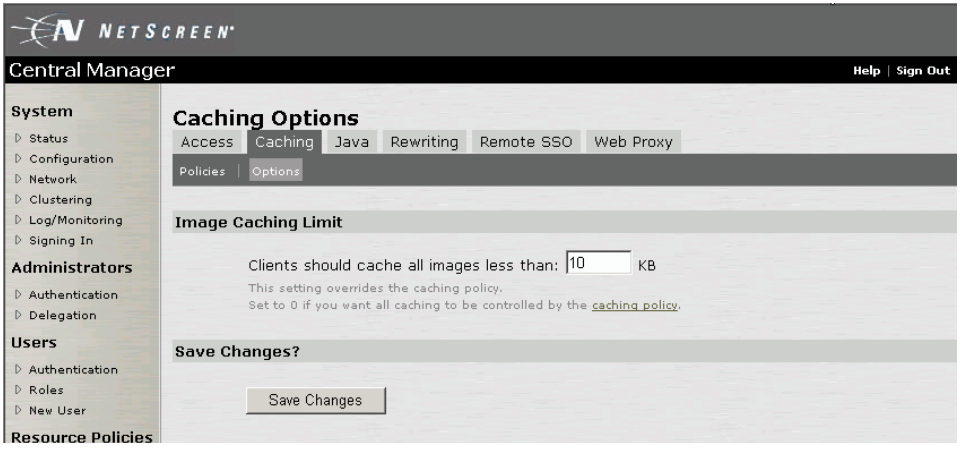


Abbildung 100:Resource Policies > Web > Caching > Options

Registerkarte „Java > Access Control“

Auf der Registerkarte **Java > Access Control** können Sie eine Webressourcenrichtlinie schreiben, die steuert, mit welchen Servern und Ports Java-Applets eine Verbindung herstellen können.

☑ Schreiben einer Ressourcenrichtlinie für die Java-Zugriffsteuerung

So schreiben Sie eine Ressourcenrichtlinie für die Java-Zugriffsteuerung:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.
2. Klicken Sie auf der Seite **Java Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow socket access**

     Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Deny socket access**

     Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Java Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Java > Code Signing“

Auf der Registerkarte **Java > Code Signing** können Sie eine Webressourcenrichtlinie schreiben, die angibt, wie das IVE Java-Applets neu schreibt. Wenn das IVE ein signiertes Java-Applet vermittelt, signiert es das Applet standardmäßig mit einem eigenen Zertifikat neu, das nicht mit einem Standardstammzertifikat verkettet ist. Wenn ein Benutzer ein Applet anfordert, das Aufgaben mit einem hohen Risikopotential durchführt, z. B. Zugreifen auf Netzwerkserver, wird im Browser des Benutzers in einer Sicherheitswarnung angezeigt, dass der Stamm nicht vertrauenswürdig ist. Um die Anzeige dieser Warnung zu vermeiden, können Sie ein Codesignaturzertifikat importieren, mit dem das IVE zu vermittelnde Applets neu signiert. Weitere Informationen zu Codesignaturzertifikaten finden Sie unter „Appletzertifikate“ auf Seite 71.

☑ Schreiben einer Ressourcenrichtlinie für die Java-Codesignatur

So schreiben Sie eine Ressourcenrichtlinie für die Java-Codesignatur:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Java > Access Control** aus.
2. Klicken Sie auf der Seite **Java Signing Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Resign applets using applet certificate**

     Erlaubt, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Resign applets using applet certificate**

     Verhindert, dass Java-Applets eine Verbindung mit den Servern (und ggf. Ports) in der Liste **Resources** herstellen.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Java Signing Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Rewriting > Selective Rewriting“

Auf der Registerkarte **Rewriting > Selective Rewriting** können Sie eine Webressourcenrichtlinie schreiben, die es Ihnen ermöglicht, eine Liste von Hosts festzulegen, für die das IVE Inhalt und Ausnahmen von der Liste vermittelt. Standardmäßig vermittelt das IVE alle Benutzeranforderungen für Webhosts, sofern Sie nicht die Anforderungsverarbeitung für bestimmte Hosts anhand eines anderen Verfahrens konfiguriert haben, z. B. Secure Application Manager.

Erstellen Sie eine Richtlinie für das selektive Neuschreiben, wenn das IVE den Datenverkehr von Websites vermitteln soll, die sich außerhalb des Firmennetzwerks befinden, z. B. „yahoo.com“, oder wenn das IVE keinen Datenverkehr für Client-/Serveranwendungen vermitteln soll, die Sie als Webressourcen bereitgestellt haben, z. B. Microsoft OWA (Outlook Web Access).

☑ Schreiben einer Ressourcenrichtlinie für selektives Neuschreiben

So schreiben Sie eine Ressourcenrichtlinie für selektives Neuschreiben:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Selective Rewriting** aus.
2. Klicken Sie auf der Seite **Web Rewriting Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Rewrite content**

     Das IVE vermittelt sämtliche Webinhalte der Ressourcen, die in der Liste **Resources** angegeben sind.
   - **Don't rewrite content**

     Das IVE vermittelt keine Webinhalte der Ressourcen, die in der Liste **Resources** angegeben sind. Wenn ein Benutzer eine Ressource anfordert, auf die diese Option zutrifft, zeigt das IVE eine Seite an, die eine Verknüpfung mit der angeforderten Ressource enthält, und der Benutzer wird aufgefordert, auf diese Verknüpfung zu klicken. Durch diese Verknüpfung wird die Ressource in einem neuen Browserfenster geöffnet, und die Seite, von der die Anforderung ursprünglich durchgeführt wurde, wird weiterhin im IVE angezeigt.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Web Rewriting Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie" auf Seite 325.

Registerkarte „Rewriting > Pass-through Proxy"

Auf der Registerkarte **Rewriting > Pass-through Proxy** können Sie eine Webressourcenrichtlinie schreiben, die Webanwendungen angibt, für die das IVE nur minimale Vermittlung übernimmt. Zum Erstellen einer Ressourcenrichtlinie für Durchgangsproxys müssen Sie zwei Angaben machen:

- Die Webanwendungen, die über den Durchgangsproxy vermittelt werden.
- Die Art der Überwachung von Clientanforderungen an die Anwendungsserver durch das IVE.

Weitere Informationen zu dieser Funktion finden Sie unter „Durchgangsproxy – Übersicht" auf Seite 103.

☑ Schreiben einer Ressourcenrichtlinie für Durchgangsproxys

So schreiben Sie eine Ressourcenrichtlinie für Durchgangsproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Rewriting > Pass-through Proxy** aus.
2. Klicken Sie auf der Seite **Pass-through Proxy Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Feld **URL** einen Hostnamen oder eine IP-Adresse für den Anwendungsserver sowie einen Port an, von dem der URL normalerweise intern auf die Anwendung zugreift.
5. Wählen Sie aus, wie die Durchgangsproxy-Funktion aktiviert werden soll:
   - **Use virtual hostname**

     Wenn Sie diese Option auswählen, müssen Sie einen Hostnamenalias für den Anwendungsserver angeben. Wenn das IVE eine Clientanforderung für den Hostnamenalias des Anwendungsservers empfängt, leitet es die Anforderung an den angegebenen Anwendungsserverport im Feld **URL** weiter.

     Wichtig: Wenn Sie diese Option auswählen, müssen Sie auf der Registerkarte **System > Network Settings > Internal Port** im Bereich **Network Identity** auch den IVE-Namen und den Hostnamen definieren.

   - **Use IVE port**

     Wenn Sie diese Option auswählen, müssen Sie einen eindeutigen IVE-Port zwischen 11000-11099 angeben. Das IVE überwacht auf dem angegebenen IVE-Port die Clientanforderungen an den Anwendungsserver und leitet diese an den Anwendungsserverport weiter, der im Feld **URL** angegeben wurde.
6. Geben Sie im Bereich **Action** die Methode an, die das IVE zum Vermitteln des Datenverkehrs verwenden soll:
   - **Rewrite XML**
   - **Rewrite external links**
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Pass-through Proxy Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Anwendung, die von einem Benutzer angefordert wurde, zu einer in der Liste **Resource** angegebenen Anwendung für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

9. Wenn Sie Folgendes auswählen:
   - **Use virtual hostname**, müssen Sie außerdem Folgendes durchführen:
     1 Hinzufügen einen Eintrags für jeden Hostnamenalias eines Anwendungsservers im externen DNS, der für das IVE aufgelöst wird.
     2 Hochladen eines Serverzertifikats mit Platzhaltern in das IVE (empfohlen).
   - **Use IVE port**, müssen Sie Datenverkehr für den IVE-Port öffnen, den Sie für den Anwendungsserver in der Firmenfirewall angegeben haben.

   Hinweis: Wenn die Anwendung mehrere Ports überwacht, konfigurieren Sie jeden Anwendungsport als separaten Durchgangsproxyeintrag mit einem separaten IVE-Port. Wenn Sie über verschiedene Hostnamen oder IP-Adressen auf den Server zugreifen möchten, müssen Sie diese Optionen einzeln konfigurieren. Sie können dann denselben IVE-Port verwenden.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Remote SSO > Form POST“

Auf der Registerkarte **Remote SSO > Form POST** können Sie eine Webressourcenrichtlinie schreiben, die Webanwendungen angibt, an die das IVE Daten sendet. In den Daten können Benutzername und Kennwort eines IVE-Benutzers und durch Systemvariablen gespeicherte Systemdaten enthalten sein. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 107.

☑ Schreiben einer Ressourcenrichtlinie für Remote-SSO Form POST

So schreiben Sie eine Ressourcenrichtlinie für Remote-SSO Form POST:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Remote SSO > Form POST** aus.
2. Klicken Sie auf der Seite **Form POST Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Perform the POST defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, führt das IVE mit den Benutzerdaten, die im Bereich **POST details** angegeben sind, einen Form-POST durch.
   - **Do NOT perform the POST defined below**

     Das IVE führt keinen Form-POST mit den Benutzerdaten durch, die im Bereich **POST details** angegeben wurden.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Geben Sie im Bereich **POST details** Folgendes an:
   - URL der Anmeldeseite der Back-End-Webanwendung. Aktivieren Sie **Deny direct login for this resource**, wenn Sie verhindern möchten, dass Benutzer direkt auf diesen URL zugreifen können.
   - Zum Senden bestimmter Benutzerdaten und Änderungsberechtigung für den Benutzer:
     - **User label** – Text, der auf der Benutzerseite **Advanced Preferences** auf dem IVE angezeigt wird. Dieses Feld ist erforderlich, wenn Sie Benutzern erlauben oder oder von ihnen fordern, Daten zu ändern, die an Back-End-Anwendungen gesendet werden.
     - **Name**– Dieser Name bezeichnet die Daten im Feld **Value**. (Dieser Name wird vermutlich von der Back-End-Anwendung erwartet.)

- **Value** – Der Wert, der für den angegebenen **Namen** an das Formular gesendet wird. Sie können statische Daten oder eine Systemvariable eingeben. Eine Liste gültiger Variablen finden Sie auf „Systemvariablen und Beispiele“ auf Seite 442.
- **User modifiable?** – Setzen Sie diese Einstellung auf **Not modifiable**, wenn Sie es Benutzern verbieten möchten, Informationen im Feld **Value** zu ändern. Setzen Sie sie auf **User CAN change value**, wenn Sie es dem Benutzer ermöglichen möchten, Daten für eine Back-End-Anwendung anzugeben. Setzen Sie diese Einstellung auf **User MUST change value**, wenn Benutzer zusätzliche Daten eingeben müssen, um auf die Back-End-Anwendung zugreifen zu können. Wenn Sie eine der letzteren Einstellungen auswählen, wird auf der Benutzerseite **Advanced Preferences** auf dem IVE ein Dateneingabefeld angezeigt. Dieses Feld wird mit dem im Feld **User label** eingegebenen Text beschriftet. Wenn Sie im Feld **Value** einen Wert angeben, wird dieser im Feld angezeigt, kann jedoch geändert werden.

8. Klicken Sie auf **Save Changes**.
9. Ordnen Sie die Richtlinien auf der Seite **Form POST Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Remote SSO > Headers/Cookies“

Auf der Registerkarte **Remote SSO > Headers/Cookies** können Sie eine Webressourcenrichtlinie schreiben, die benutzerdefinierte Webanwendungen angibt, an die das IVE Header und Cookies sendet. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 107.

☑ Schreiben einer Ressourcenrichtlinie für SSO-Header und -Cookies

So schreiben Sie eine Ressourcenrichtlinie für SSO-Header/Cookies:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Remote SSO > Headers/Cookies** aus.
2. Klicken Sie auf der Seite the **Headers/Cookies Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Append headers as defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, an den angegebenen URL.
   - **Do NOT append headers as defined below**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, nicht an den angegebenen URL.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Geben Sie im Bereich **Headers and values** Folgendes an:
   - **Header name** – Text, den das IVE als Headerdaten sendet.
   - **Value** – Wert für den angegebenen Header.
8. Klicken Sie auf **Save Changes**.
9. Ordnen Sie die Richtlinien auf der Seite **Headers/Cookies Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Web Proxy > Policies“

Auf der Registerkarte **Web Proxy > Policies** können Sie eine Webressourcenrichtlinie schreiben, die benutzerdefinierte Webanwendungen angibt, an die das IVE Header und Cookies sendet. Weitere Informationen zu dieser Funktion finden Sie unter „Remote SSO – Übersicht“ auf Seite 107.

☑ Schreiben einer Ressourcenrichtlinie für Webproxys

So schreiben Sie eine Ressourcenrichtlinie für Webproxys:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Web Proxy > Policies** aus.
2. Klicken Sie auf der Seite **Web Proxy Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)

4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Webressourcen“ auf Seite 46.

Wichtig: Das IVE löst keine Domänennamen in IP-Adressen auf und führt kein Reverse-Lookup für IP-Adressen durch. Ein URL, der auf eine IP-Adresse und nicht auf einen Hostnamen verweist, wird nur durchgelassen, wenn ein entsprechender Eintrag für die IP-Adresse in der Liste **Resources** vorhanden ist.

---

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Access web resources directly**

     Das IVE vermittelt die Anforderung des Benutzers an einen Back-End-Server und die Antwort des Servers an den Benutzer. Dies gilt für Anforderungen an eine Ressource, die in der Liste **Resources** angegeben ist.
   - **Access web resources through a web proxy**

     Wenn ein Benutzer den Zugriff auf eine Ressource anfordert, die in der Liste **Resources** aufgeführt ist, sendet das IVE die Benutzerdaten, die im Bereich **POST details** angegeben sind, nicht an den angegebenen URL. Wenn Sie diese Option auswählen, müssen Sie die Einstellungen für den Webproxy angeben. Weitere Informationen finden Sie unter „Registerkarte „Web Proxy > Settings““ auf Seite 348.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Headers/Cookies Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert

wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Ein Beispiel für eine Webressourcenrichtlinie finden Sie in den Abbildungen unter „Schreiben einer Webressourcenrichtlinie“ auf Seite 325.

Registerkarte „Web Proxy > Settings“

Sie können alle vom IVE durchgeführten Webanforderungen an einen Webproxy leiten, statt mit dem IVE eine direkte Verbindung mit den Webservern herzustellen. Diese Funktion bietet sich an, wenn Ihre Richtlinien für die Netzwerksicherheit diese Konfiguration erfordern oder wenn Sie zur Leistungssteigerung einen Webproxy mit Zwischenspeicherung verwenden möchten.

Gegenwärtig gilt für das IVE Folgendes:

- Das IVE unterstützt nur HTTP-Proxys, HTTPS-Proxys (Secure-HTTP) werden nicht unterstützt. Das IVE ruft Secure-HTTP-Inhalte über eine direkte Verbindung ab.
- Authentifizierung über Webproxys wird nicht unterstützt. Wenn Sie die Webproxyfunktion des IVE verwenden möchten, müssen Sie Ihren Webproxy so konfigurieren, dass nicht authentifizierte Benutzer akzeptiert werden.

☑ Angeben von Einstellungen für Webproxys

Auf der Registerkarte **Web Proxy** können Sie Einstellungen für den Webproxy angeben.

So geben Sie Einstellungen für den Webproxy an:

1. Wählen Sie in der Webkonsole **Resource Policies > Web > Web Proxy > Settings** aus.
2. Geben Sie unter **Web Proxy Server Information** den Namen oder die IP-Adresse des Webproxyservers sowie die Portnummer ein, an der der Proxyserver Daten abfragt.
3. Aktivieren Sie unter **Unqualified hostnames** das Kontrollkästchen **Send requests specified without a domain name to the Web proxy**, falls URLs mit unvollständigen Hostnamen, wie zum Beispiel `http://host/xyz` anstelle von `http://host.domain.com/xyz`, an den Proxyserver weitergeleitet werden sollen.
4. Klicken Sie auf **Save Changes**.

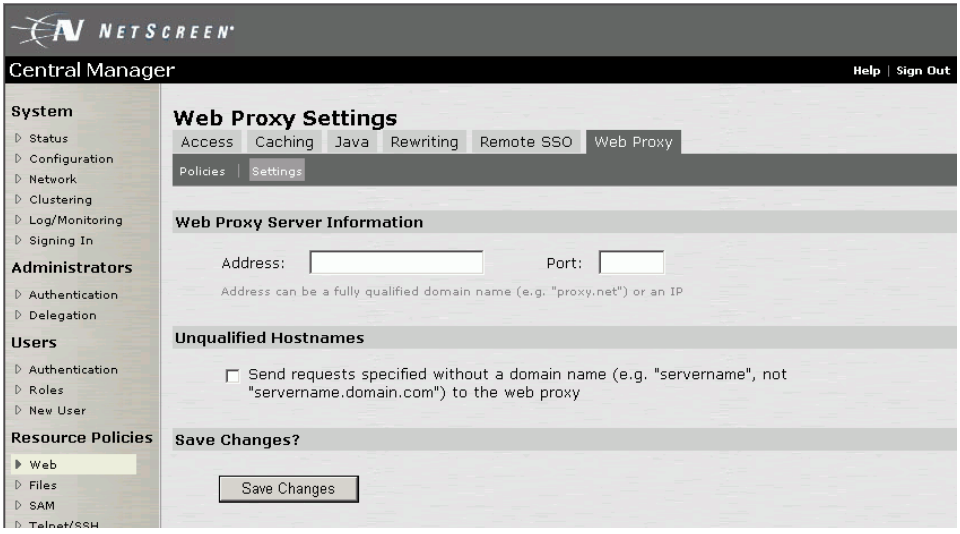


Abbildung 101:Resource Policies > Web > Web Proxy > Settings

Konfigurieren der Seite „Files“

Die Seite **Resource Policies > Files** enthält die folgenden Registerkarten:

Registerkarte „Windows > Access“ 352
Registerkarte „Windows > Credentials“ 355
Registerkarte „UNIX/NFS“ 358
Registerkarte „Encoding“ 360

Auf der Seite **Resource Policies > Files** können Sie Folgendes durchführen:

Schreiben einer Ressourcenrichtlinie für Windows-Zugriff 352
Schreiben einer Ressourcenrichtlinie für Windows-Anmeldeinformationen 355
Schreiben einer UNIX/NFS-Ressourcenrichtlinie 358
Angeben der Codierung für die Internationalisierung von IVE-Datenverkehr 360

Schreiben einer Dateiressourcenrichtlinie

Wenn Sie die Dateizugriffsfunktion für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Windows- und UNIX/NFS-Ressourcen ein Benutzer zugreifen darf und welche Codierung für die Kommunikation mit Windows- und NFS-Dateifreigaben verwendet werden soll. Wenn ein Benutzer eine Datei anfordert, wertet das IVE die entsprechenden Ressourcenrichtlinien aus, z.B. Ressourcenrichtlinien für den Windows-Zugriff bei einer Anforderung eines MS Word-Dokuments (DOC-Datei). Wenn das IVE für eine Benutzeranforderung einer Ressource, die in der entsprechenden Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Dateiressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Dateirichtlinie müssen Sie Dateiserver oder bestimmte Freigaben angeben. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48 und „Angeben von UNIX/NFS-Dateiressourcen“ auf Seite 49.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.

- **Aktionen:** Jeder Typ von Ressourcenrichtlinie führt eine bestimmte Aktion aus: Zugriff auf eine Ressource gewähren bzw. verweigern oder eine Funktion ausführen bzw. nicht ausführen, z.B. einem Benutzer Schreibzugriff auf ein Verzeichnis zu gewähren. Sie können auch detaillierte Regeln schreiben, mit denen Sie weitere Bedingungen für eine Benutzeranforderung festlegen. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

Registerkarte „Windows > Access“

Über die Registerkarte **Windows > Access** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche Windows-Ressourcen Benutzer zugreifen dürfen. Für Windows-Ressourcen geben Sie den Server und die Freigabe sowie bei Bedarf den Pfad für einen bestimmten Ordner ein.

☑ Schreiben einer Ressourcenrichtlinie für Windows-Zugriff

So schreiben Sie eine Ressourcenrichtlinie für Windows-Zugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Windows > Access** aus.
2. Klicken Sie auf der Seite **Windows File Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

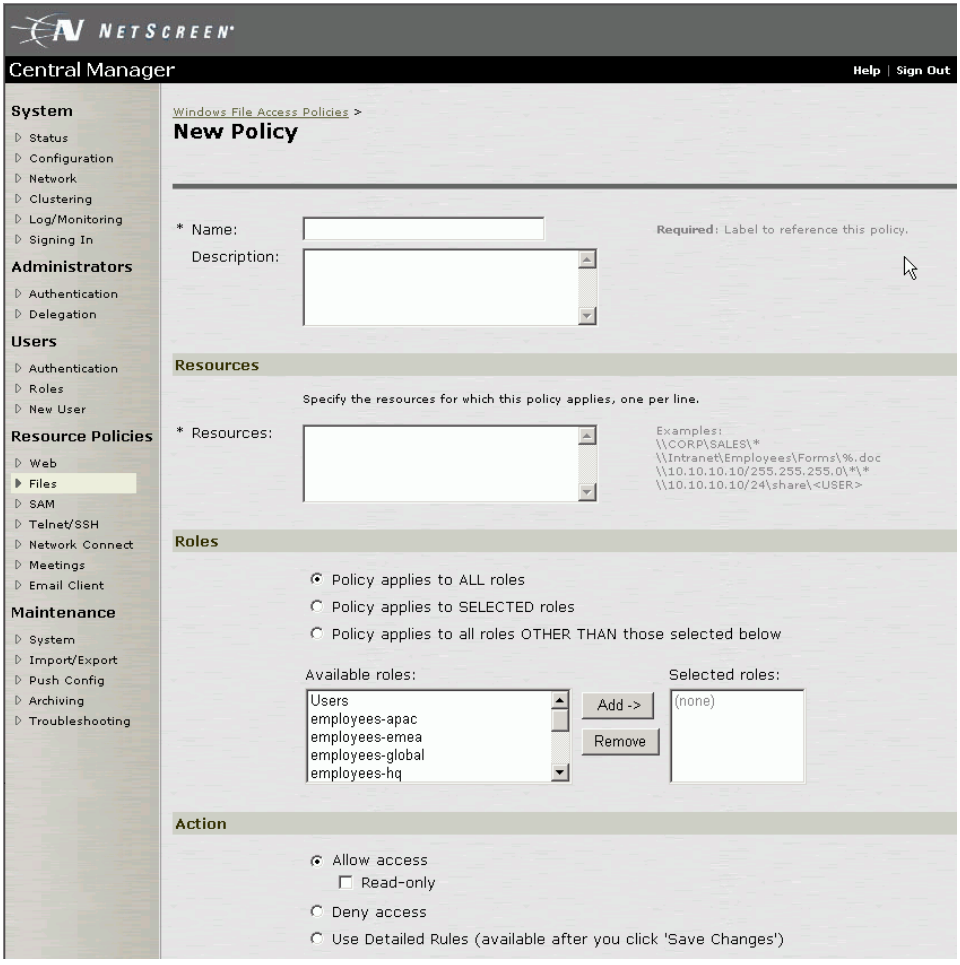


Abbildung 102:Resource Policies > Files > Windows > Access > New Policy

Registerkarte „Windows > Credentials“

Auf der Registerkarte **Windows > Credentials** können Sie eine Dateiressourcenrichtlinie schreiben, mit der Sie Anmeldeinformationen für das IVE angeben können, die an einen Dateiserver gesendet werden, wenn eine Benutzeranfrage einer Ressource in der Liste **Resource** entspricht. Sie können außerdem das IVE so konfigurieren, dass Benutzer zur Eingabe ihrer Anmeldeinformationen aufgefordert werden.

☑ Schreiben einer Ressourcenrichtlinie für Windows-Anmeldeinformationen

So schreiben Sie eine Ressourcenrichtlinie für Windows-Anmeldeinformationen:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Windows > Credentials** aus.
2. Klicken Sie auf der Seite **Windows Credentials Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Windows-Dateiressourcen“ auf Seite 48.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Use specified credentials**

     Mithilfe dieser Option können Sie Administrator-Anmeldeinformationen angeben, die das IVE an die Ressourcen sendet, die auf Ordner- und Dateiebene in der Liste **Resources** angegeben ist. Der IVE-Server für die Dateinavigation hält jedoch die Verbindungen mit einem Ser-

ver\Freigabe offen, sodass die Verbindung mit einem anderen Ordner auf derselben Freigabe über ein anderes Konto möglicherweise nicht zuverlässig funktioniert. Wenn die angegebenen Anmeldeinformationen nicht funktionieren, fordert das IVE den Benutzer auf, die Anmeldeinformationen auf einer zwischengeschalteten Seite einzugeben.

- **Prompt for user credentials**

  Wenn für eine freigegebene Datei, die in der Liste **Resources** angegeben ist, Anmeldeinformationen erforderlich sind, vermittelt das IVE die Anfrage, indem eine Authentifizierungsanfrage auf dem IVE angezeigt wird. Der Benutzer muss die Anmeldeinformationen für die Freigabe eingeben, auf die er zugreifen möchte.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Windows File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

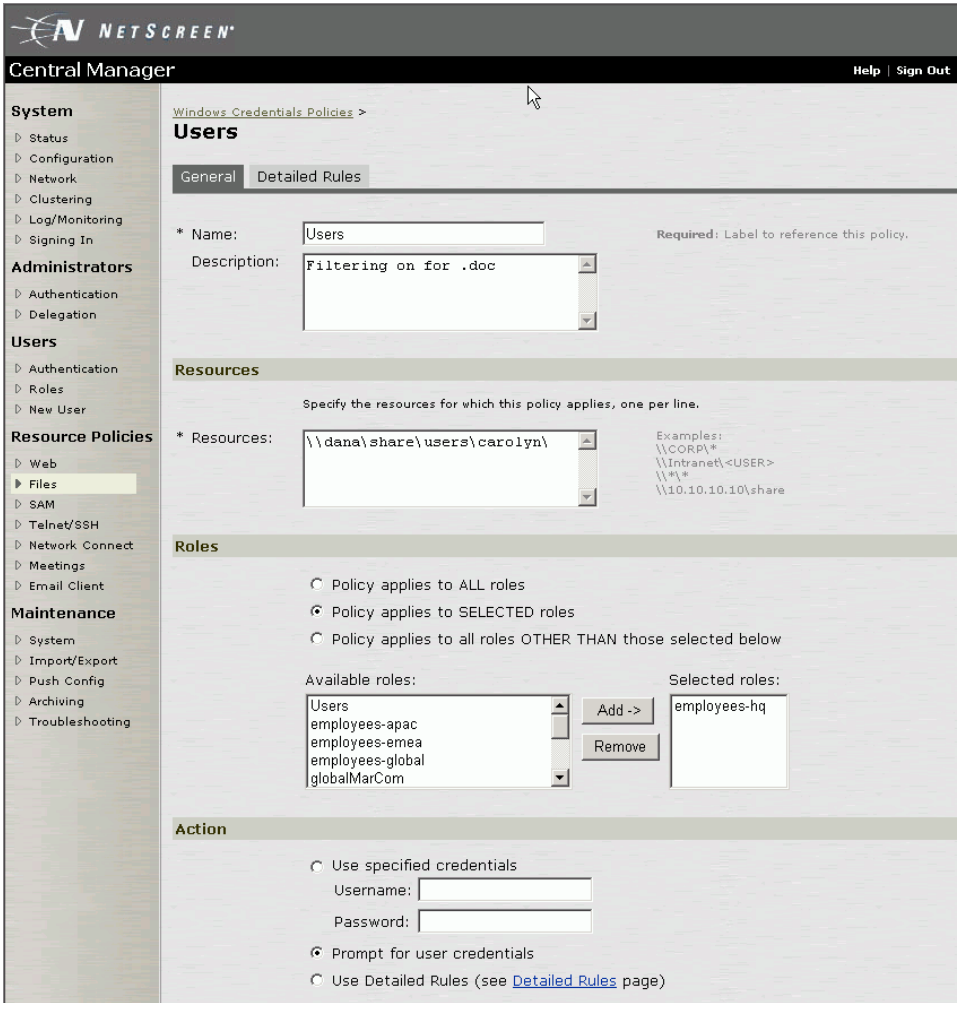


Abbildung 103:Resource Policies > Files > Windows > Credentials > New Policy

Registerkarte „UNIX/NFS“

Über die Registerkarte **UNIX/NFS** können Sie eine Dateiressourcenrichtlinie schreiben, die angibt, auf welche UNIX/NFS-Ressourcen Benutzer zugreifen dürfen. Sie geben UNIX/NFS-Ressourcen an, indem Sie einen Serverhostnamen oder die IP-Adresse eingeben und bei Bedarf den Pfad zu einer bestimmten Freigabe angeben.

☑ Schreiben einer UNIX/NFS-Ressourcenrichtlinie

So schreiben Sie eine UNIX/NFS-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole **Resource Policies > File > UNIX/NFS** aus.
2. Klicken Sie auf der Seite **Unix/NFS File Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von UNIX/NFS-Dateiressourcen“ auf Seite 49.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind. Aktivieren Sie **Read-only**, damit die Benutzer keine Dateien auf dem Server speichern können.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.

- **Use Detailed Rules**

  Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.

7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Unix/NFS File Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

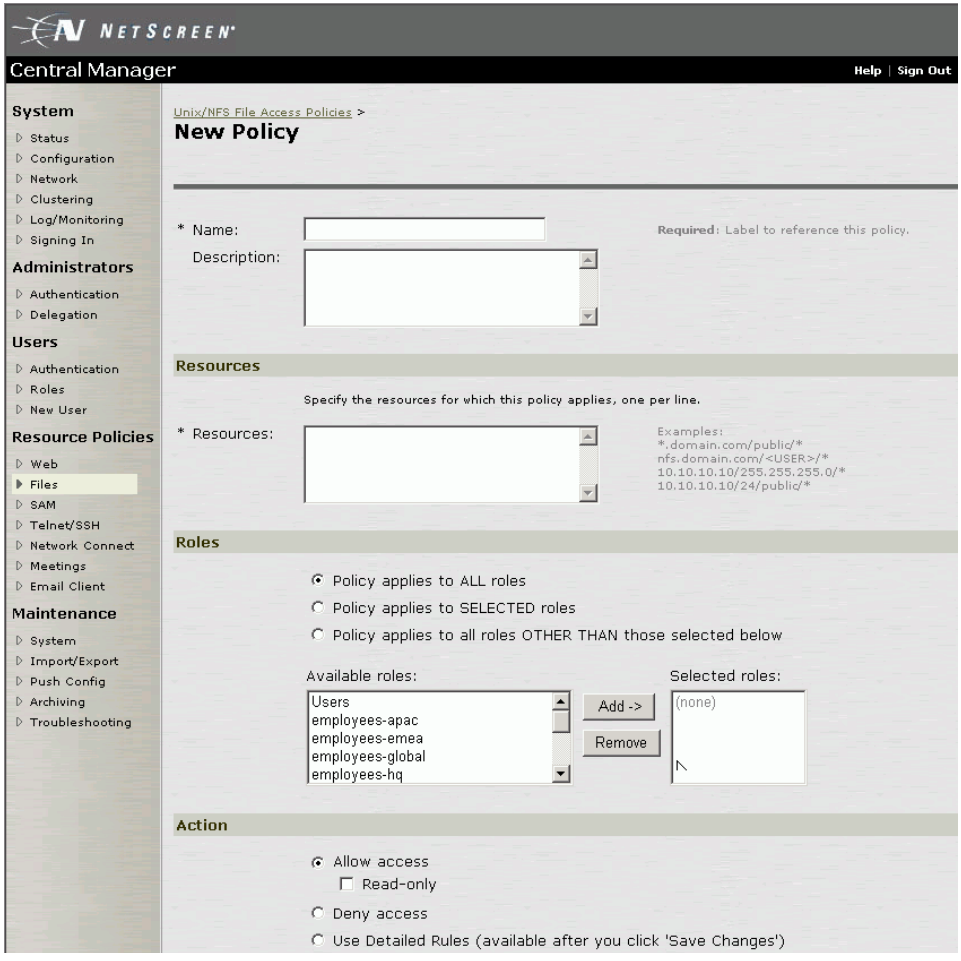


Abbildung 104:Resource Policies > Files > UNIX/NFS > New Policy

Registerkarte „Encoding“

Auf der Registerkarte **Files > Encoding** können Sie festlegen, wie das IVE die Daten bei der Interaktion mit Dateiservern codiert.

☑ Angeben der Codierung für die Internationalisierung von IVE-Datenverkehr

So geben Sie die Codierung für die Internationalisierung von IVE-Datenverkehr an:

1. Wählen Sie in der Webkonsole **Resource Policies > File > Encoding** aus.
2. Wählen Sie die entsprechende Option aus:
   - Western European (ISO-8859-1)
   - Japanese (Shift-JIS)
   - Korean
3. Klicken Sie auf **Save Changes**.

Abbildung 105:Resource Polices > Files > Encoding

Konfigurieren der Seite „SAM“

Auf der Seite **Resource Policies > SAM** können Sie Folgendes durchführen:

Schreiben einer Ressourcenrichtlinie für Secure Application Manager 362

Mithilfe der Aktualisierungsoption Secure Application Manager können Benutzer über einen verschlüsselten SSL-Tunnel auf Anwendungsserver zugreifen, als ob sie sich im Firmen-LAN befänden. Weitere Informationen finden Sie unter „Secure Application Manager – Übersicht“ auf Seite 109.

Schreiben einer SAM-Ressourcenrichtlinie

Wenn Sie die Zugriffsfunktion Secure Application Manager für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die die Anwendungsserver angeben, auf die die Benutzer zugreifen dürfen. Diese Richtlinien gelten sowohl für die Java- als auch für die Windows-Version von Secure Application Manager (J-SAM bzw. W-SAM). Wenn ein Benutzer eine Anforderung für einen Anwendungsserver vornimmt, wertet das IVE die SAM-Ressourcenrichtlinien aus. Wenn das IVE für eine Benutzeranforderung für eine Ressource, die in einer SAM-Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer SAM-Ressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer SAM-Richtlinie müssen Sie Anwendungsserver angeben, mit denen Benutzer eine Verbindung herstellen können.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen. SAM-Ressourcenrichtlinien gelten für alle Benutzeranforderungen, die anhand der Versionen J-SAM oder W-SAM vorgenommen wurden.
- **Aktionen:** Eine Ressourcenrichtlinie für Secure Application Manager erlaubt oder verweigert den Zugriff auf einen Anwendungsserver.

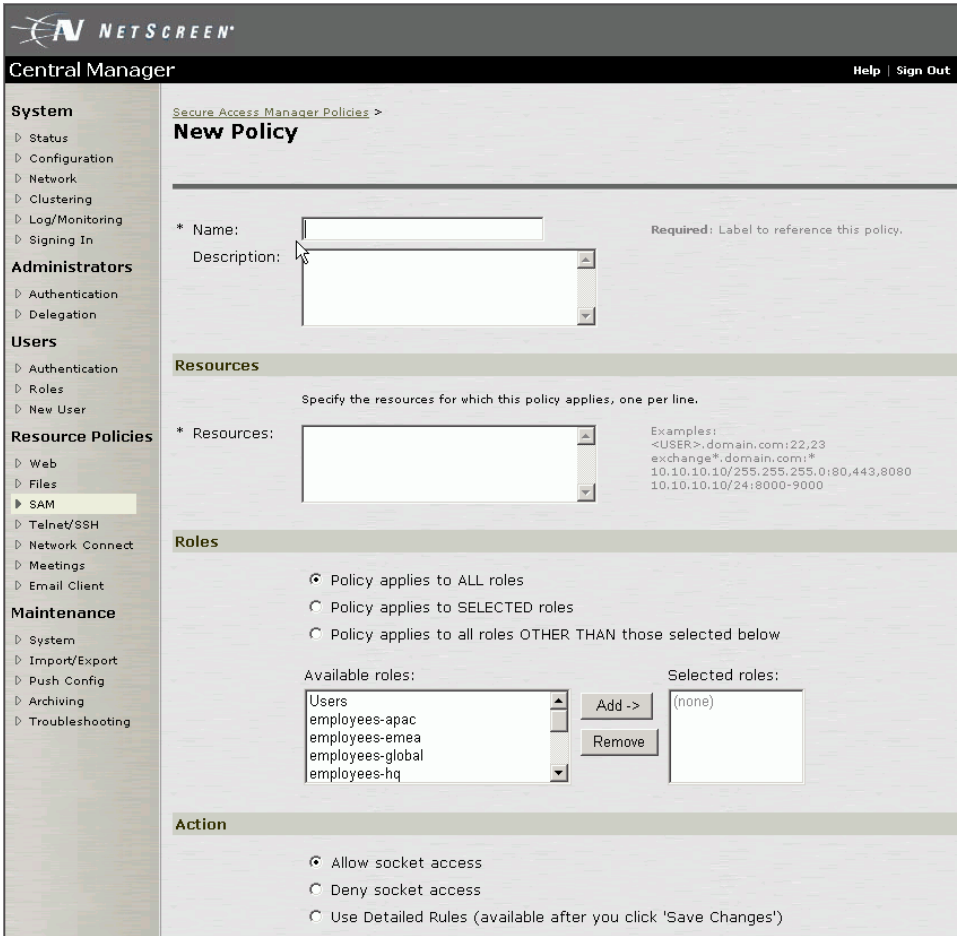


Abbildung 106:Resource Policies > SAM > New Policy

☑ Schreiben einer Ressourcenrichtlinie für Secure Application Manager

So schreiben Sie eine Ressourcenrichtlinie für Secure Application Manager:

1. Wählen Sie in der Webkonsole **Resource Policies > SAM** aus.
2. Klicken Sie auf der Seite **Secure Application Manager Policies** auf **New Policy**.

3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1 Eine Bezeichnung für diese Richtlinie.
   2 Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Anwendungsserver an, für die diese Richtlinie gelten soll.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow socket access**

     Hiermit erlauben Sie den Zugriff auf die Anwendungsserver, die in der Liste **Resources** aufgeführt sind.
   - **Deny socket access**

     Hiermit verweigern Sie den Zugriff auf die Anwendungsserver, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Secure Application Manager Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Konfigurieren der Seite „Telnet/SSH“

Auf der Seite **Resource Policies > Telnet/SSH** können Sie Folgendes durchführen:

Schreiben einer Telnet/SSH-Ressourcenrichtlinie.....366

Mithilfe der Aktualisierungsoption sicherer Terminalzugriff können Benutzer eine unverschlüsselte Verbindung mit internen Serverhosts über Telnet-Protokolle herstellen oder in einer verschlüsselten SSH-Sitzung (Secure Shell) über eine webbasierte Terminalsitzungs-Emulation kommunizieren. Diese Funktion unterstützt die folgenden Anwendungen und Protokolle:

- Netzwerkprotokolle
  - Telnet
  - SSH
- Terminaleinstellungen
  - VT100, VT320 und Ableitungen
  - Bildschirmpuffer
- Sicherheit
  - Web-/Clientsicherheit über SSL
  - Hostsicherheit: SSH (sofern erwünscht)

Schreiben einer Telnet/SSH-Ressourcenrichtlinie

Wenn Sie die Zugriffsfunktion Telnet/SSH für eine Rolle aktivieren, müssen Sie Ressourcenrichtlinien erstellen, die die Remoteserver angeben, auf die die Benutzer zugreifen dürfen. Wenn das IVE für eine Benutzeranforderung für eine Ressource, die in einer Telnet/SSH-Richtlinie aufgeführt ist, eine Übereinstimmung findet, führt es die für die Ressource angegebene Aktion aus.

Beim Schreiben einer Telnet/SSH-Ressourcenrichtlinie müssen Sie die folgenden zentralen Informationen angeben:

- **Ressourcen:** Eine Ressourcenrichtlinie muss mindestens eine Ressource angeben, auf die sich die Richtlinie bezieht. Beim Schreiben einer Telnet/SSH-Richtlinie müssen Sie Remoteserver angeben, mit denen Benutzer eine Verbindung herstellen können.
- **Rollen:** Eine Ressourcenrichtlinie muss die Rollen angeben, auf die sie sich bezieht. Wenn ein Benutzer eine Anforderung durchführt, ermittelt das IVE zunächst die für die Rolle gültigen Richtlinien und wertet dann die Richtlinien aus, die auf die Anforderung zutreffen.

- **Aktionen:** Eine Telnet/SSH-Ressourcenrichtlinie erlaubt oder verweigert den Zugriff auf einen Server.

☑ Schreiben einer Telnet/SSH-Ressourcenrichtlinie

So schreiben Sie eine Telnet/SSH-Ressourcenrichtlinie:

1. Wählen Sie in der Webkonsole **Resource Policies > Telnet/SSH** aus.
2. Klicken Sie auf der Seite **Telnet/SSH Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Server an, für die diese Richtlinie gelten soll.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Server, die in der Liste **Resources** aufgeführt sind.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Server, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit geben Sie eine oder mehrere detaillierte Regeln für diese Richtlinie an. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel“ auf Seite 52.
7. Klicken Sie auf **Save Changes**.

8. Ordnen Sie die Richtlinien auf der Seite **Telnet/SSH Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

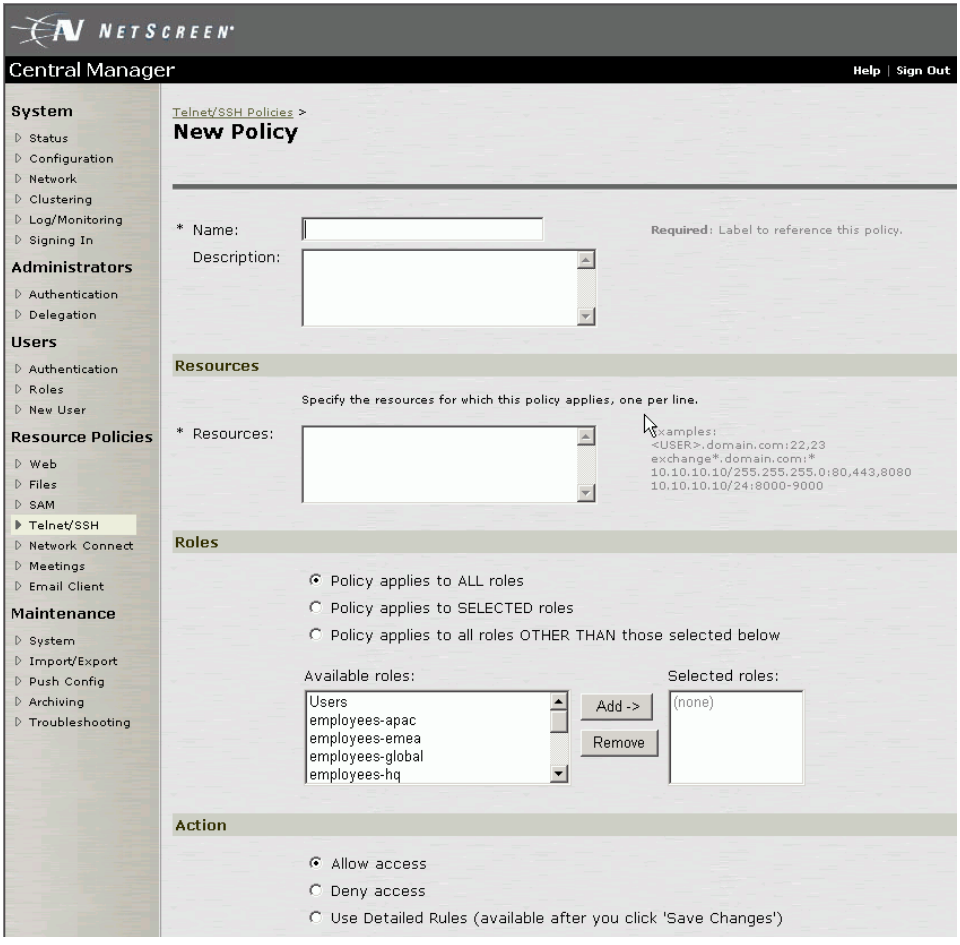


Abbildung 107:Resource Policies > Telnet/SSH > New Policy

Konfigurieren der Seite „Network Connect“

Über die Aktualisierungsoption Network Connect verfügen Sie auf Netzwerkebene über einen sicheren, SSL-basierten Remotezugriff auf ***alle*** Unternehmens-Anwendungsressourcen über das IVE.

Wichtig: Benutzer müssen auf ihrem Windows PC über Administrator- oder Hauptbenutzerberechtigungen verfügen, um das IVE für die Installation des Network Connect-Agent zu aktivieren.

Die Seite **Resource Policies > Network Connect** enthält die folgenden Registerkarten:

Registerkarte „Access“ 370
Registerkarte „IP Address Pools“ 373

Auf der Seite **Resource Policies > Network Connect** können Sie Folgendes durchführen:

Schreiben einer Ressourcenrichtlinie für Network Connect-Zugriff: 370
Schreiben einer Network Connect-Ressourcenrichtlinie für IP-Adresspools 373

Konfigurieren von Network Connect

Wenn Sie die Zugriffsfunktion Network Connect für eine Rolle konfigurieren, müssen Sie Ressourcenrichtlinien erstellen, die angeben, auf welche Ressourcen ein Benutzer zugreifen darf und von welchen IP-Pools das IVE dem Network Connect-Client-Agent und dem Serverprozess IP-Adressen zuweisen kann. Außerdem müssen Sie den Router so konfigurieren, dass dieser auf die IP-Adresse des internen Ports des IVE als Gateway für Routen von Antworten auf Clientanforderungen über das Netzwerk weist.

Anforderungen für Cluster

Wenn Sie einen Multisite-Cluster ausführen und für jeden Knoten unterschiedliche Netzwerkadressen verwendet werden, müssen Sie folgende Schritte ausführen:

- Konfigurieren Sie eine Richtlinie für IP-Adresspools für die unterschiedlichen Netzwerkadressen, die von den einzelnen Knoten im Cluster verwendet werden.
- Geben Sie für jeden Knoten im Cluster einen IP-Filter an, der nur die für den Knoten verfügbaren Netzwerkadressen herausfiltert.

- Erstellen Sie für den Router einen Zeiger für die IP-Adresse des internen Ports jedes Clusterknotens. Alle vom Router angegebenen IP-Adressen müssen sich im gleichen Subnetzwerk befinden wie der jeweilige Clusterknoten.

Registerkarte „Access“

Über die Registerkarte **Access** können Sie eine Network Connect-Ressourcenrichtlinie schreiben, die angibt, mit welchen Ressourcen Benutzer über Network Connect eine Verbindung herstellen dürfen.

☑ Schreiben einer Ressourcenrichtlinie für Network Connect-Zugriff:

So schreiben Sie eine Ressourcenrichtlinie für Network Connect-Zugriff:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > Access** aus.
2. Klicken Sie auf der Seite **Network Connect Access Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie im Bereich **Resources** die Ressourcen an, für die diese Richtlinie gelten soll. Weitere Informationen finden Sie unter „Angeben von Serverressourcen“ auf Seite 50.
5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.

6. Geben Sie im Bereich **Action** Folgendes an:
   - **Allow access**

     Hiermit erlauben Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Deny access**

     Hiermit verweigern Sie den Zugriff auf die Ressourcen, die in der Liste **Resources** aufgeführt sind.
   - **Use Detailed Rules**

     Hiermit definieren Sie Regeln für Ressourcenrichtlinien, die die angegebenen Ressourcen zusätzlich einschränken. Weitere Informationen finden Sie unter „Schreiben einer detaillierten Regel" auf Seite 52.
7. Klicken Sie auf **Save Changes**.
8. Ordnen Sie die Richtlinien auf der Seite **Network Connect Access Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

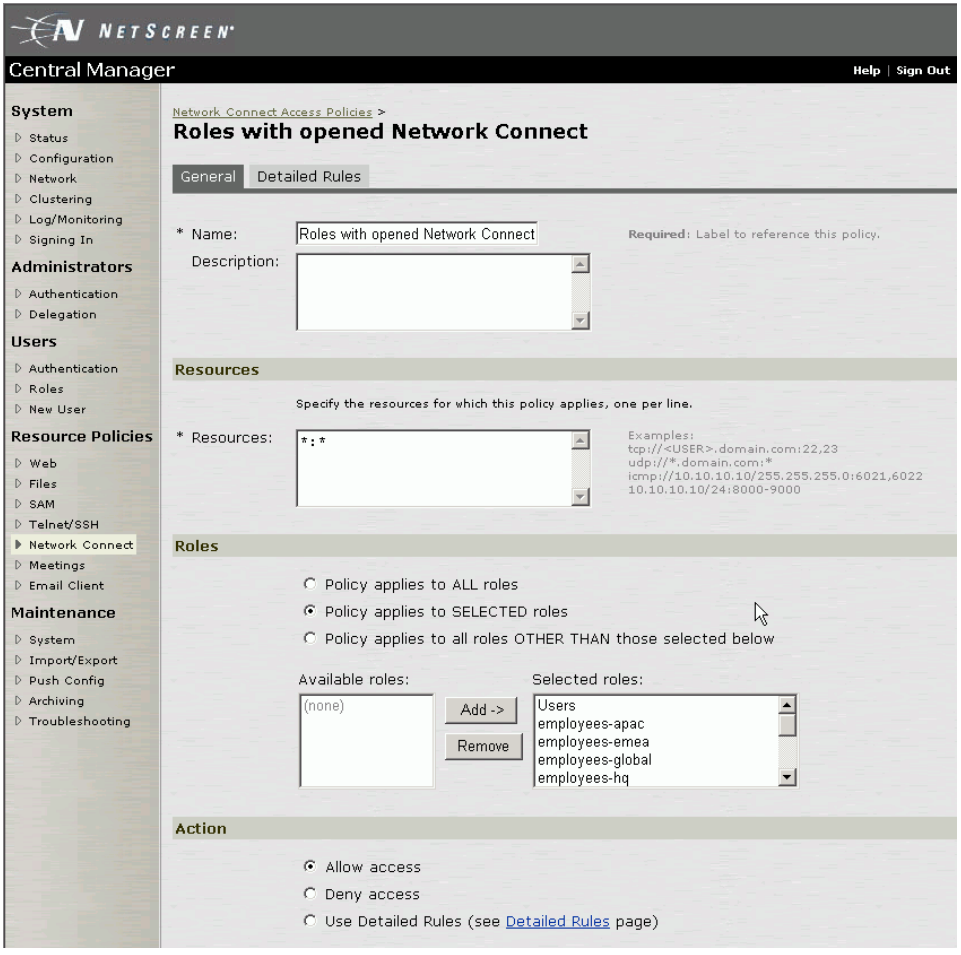


Abbildung 108: Resource Policies > Network Connect > Access > *Ausgewählte Richtlinie* > General

Registerkarte „IP Address Pools“

Über die Registerkarte **IP Address Pools** können Sie eine Network Connect-Ressourcenrichtlinie schreiben, die einen IP-Pool angibt, aus dem das IVE den Server- und Clientprozessen für eine Network Connect-Sitzung eine IP-Adresse zuweist. Wenn ein IVE eine Clientanforderung zum Starten einer Network Connect-Sitzung empfängt, weist es sowohl dem clientseitigen Network Connect-Agent als auch dem serverseitigen IVE-Prozess eine IP-Adresse zu. Die Zuweisung der IP-Adressen erfolgt anhand der Richtlinien für den IP-Adresspool, die auf eine Benutzerrolle zutreffen.

Knoten in einem Cluster mit mehreren Sites nutzen die Konfigurationsinformationen gemeinsam, d.h., dass IVEs in verschiedenen Netzwerken einen IP-Pool gemeinsam nutzen. Da jeder IVE-Knoten die Clientanforderung zum Starten der Network Connect-Sitzung empfangen kann, müssen Sie für Knoten einen IP-Filter angeben, der lediglich die für den betreffenden Knoten verfügbaren Netzwerkadressen herausfiltert. Wenn der Clusterknoten eine Anforderung zum Erstellen einer Network Connect-Sitzung empfängt, weist er aus dem gefilterten IP-Pool die zwei IP-Adressen für die Sitzung zu.

☑ Schreiben einer Network Connect-Ressourcenrichtlinie für IP-Adresspools

So schreiben Sie eine Network Connect-Ressourcenrichtlinie für IP-Adresspools:

1. Wählen Sie in der Webkonsole **Resource Policies > Network Connect > IP Address Pools** aus.
2. Klicken Sie auf der Seite **Network Connect IP Address Policies** auf **New Policy**.
3. Geben Sie auf der Seite **New Policy** Folgendes ein:
   1. Eine Bezeichnung für diese Richtlinie.
   2. Eine Beschreibung der Richtlinie. (Optional.)
4. Geben Sie unter **Resources** IP-Adressen oder einen IP-Adress-Bereich an, die das IVE Clients zuweisen soll, die den Network Connect-Dienst ausführen. Informationen zum Angeben eines IP-Bereichs finden Sie unter „Angeben von IP-Adresspools“ auf Seite 51.

Da das IVE pro Network Connect-Sitzung zwei IP-Adressen reserviert, müssen Sie eine gerade Anzahl von IP-Adressen angeben. Um z. B. eine Network Connect-Sitzung in einem IVE zuzulassen, geben Sie zwei IP-Adressen an. Um 100 Sitzungen zuzulassen, geben Sie 200 IP-Adressen an.

Hinweis: Wenn in einem LAN oder WAN einen Multi-Unit-Cluster ausführen, muss der IP-Pool Adressen enthalten, die für jeden Knoten im Cluster gültig sind. Konfigurieren Sie dann einen IP-Filter für jeden Knoten, der auf diesen IP-Pool angewendet werden soll.

---

5. Geben Sie im Bereich **Roles** Folgendes an:
   - **Policy applies to ALL roles**

     Hiermit gilt die Richtlinie für alle Benutzer.
   - **Policy applies to SELECTED roles**

     Hiermit gilt die Richtlinie nur für Benutzer, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
   - **Policy applies to all roles OTHER THAN those selected below**

     Hiermit gilt die Richtlinie für alle Benutzer *außer* den Benutzern, die zu Rollen in der Liste **Selected roles** zugeordnet sind. Dieser Liste müssen Rollen aus der Liste **Available roles** hinzugefügt werden.
6. Klicken Sie auf **Save Changes**.
7. Ordnen Sie die Richtlinien auf der Seite **Network Connect IP Address Policies** in der Reihenfolge an, in der sie vom IVE ausgewertet werden sollen. Hinweis: Wenn das IVE die Ressource, die von einem Benutzer angefordert wurde, zu einer Ressource in der Liste **Resource** für eine Richtlinie (oder ausführliche Regel) zuordnet, führt es die angegebene Aktion aus und beendet die Richtlinienverarbeitung.

Konfigurieren der Seite „Meetings“

Auf der Seite **Resource Policies > Meetings** können Sie Folgendes durchführen:

Schreiben einer Ressourcenrichtlinie für E-Mail-Benachrichtigungen von Secure Meeting.....376

Mithilfe der Aktualisierungsoption Secure Meeting können Benutzer innerhalb des gesamten Unternehmens Onlinekonferenzen über eine intuitiv bedienbare Webseite planen und abhalten. Weitere Informationen finden Sie unter „Secure Meeting – Übersicht“ auf Seite 13.

Schreiben einer Ressourcenrichtlinie für Secure Meeting

Wenn Sie die Zugriffsfunktion Secure Meeting für eine Rolle aktivieren, müssen Sie eine Ressourcenrichtlinie erstellen, die angibt, ob für Secure Meeting-Gäste automatische E-Mail-Benachrichtigungen aktiviert werden sollen. Im Gegensatz zu anderen Zugriffsfunktionen verfügt Secure Meeting nur über eine Ressourcenrichtlinie, die für *alle* Rollen gilt, für die diese Funktion aktiviert ist. Wenn Sie automatische E-Mail-Benachrichtigungen für Gäste aktivieren, müssen Sie für das Routing von Konferenz-E-Mails einen SMTP-Server verwenden, auf den das IVE zugreifen kann.

Wichtig:

Wenn Sie einen SMTP-Server für die Verwendung mit Secure Meeting aktivieren, müssen Sie auf der Registerkarte **System > Network > Internal Port** im Bereich **Network Identity** auch einen virtuellen Hostnamen für die IVE-Appliance festlegen. Secure Meeting verwendet den angegebenen Namen zum Einfügen der Konferenz-URLs in Benachrichtigungs-E-Mails und für SMTP-Aufrufe. Wenn dem IVE verschiedene Namen zugeordnet sind und Sie keinen **Virtual Hostname** angeben, müssen Sie vor dem Erstellen einer Konferenz u.U. einschränken, unter welchem Namen sich Benutzer anmelden können. Beispiel: Wenn das IVE einem internen Namen zugeordnet ist (wie **vertrieb.acmegizmo.com**), der nur innerhalb der Firmenfirewall gültig ist, sowie einem weiteren Namen (wie **partner.acmegizmo.com**), der überall verwendet werden kann, sollten sich IVE-Benutzer vor dem Erstellen einer Konferenz unter **partner.acmegizmo.com** anmelden. Andernfalls erhalten Gäste ohne IVE E-Mal-Benachrichtigungen, in denen Verknüpfungen mit einem nicht erreichbaren IVE enthalten sind.

☑ Schreiben einer Ressourcenrichtlinie für E-Mail-Benachrichtigungen von Secure Meeting

So schreiben Sie eine Ressourcenrichtlinie für E-Mail-Benachrichtigungen von Secure Meeting:

1. Wählen Sie in der Web console **Resource Policies > Meetings** aus.
2. Wählen Sie **Enabled** aus.
3. Geben Sie im Feld **SMTP Server** die IP-Adresse oder den Hostnamen eines SMTP-Servers ein, der E-Mail-Nachrichten von der Appliance an die Konferenzgäste weiterleiten kann.
4. Geben Sie bei entsprechender Anforderung vom SMTP-Server in den Feldern **SMTP Login** und **SMTP Password** einen gültigen Anmeldenamen und ein Kennwort für den angegebenen SMTP-Mail-Server ein.
5. Geben Sie im Feld **SMTP Email** Ihre E-Mail-Adresse oder die Adresse eines anderen Administrators ein. Secure Meeting verwendet die angegebene Adresse als E-Mail-Adresse des Absenders, wenn der Ersteller der E-Mail-Nachricht im NetScreen Instant Virtual Extranet keine eigene E-Mail-Adresse konfiguriert hat.
6. Klicken Sie auf **Save Changes**.
7. Konfigurieren Sie Secure Meeting-Einstellungen für einzelne Rollen anhand der Anweisungen in „Registerkarte „Meetings““ auf Seite 317.

So deaktivieren Sie automatische E-Mail-Benachrichtigungen für Konferenzgäste:

1. Wählen Sie in der Web console **Resource Policies > Meetings** aus.
2. Wählen Sie **Disabled** aus.
3. Klicken Sie auf **Save Changes**.

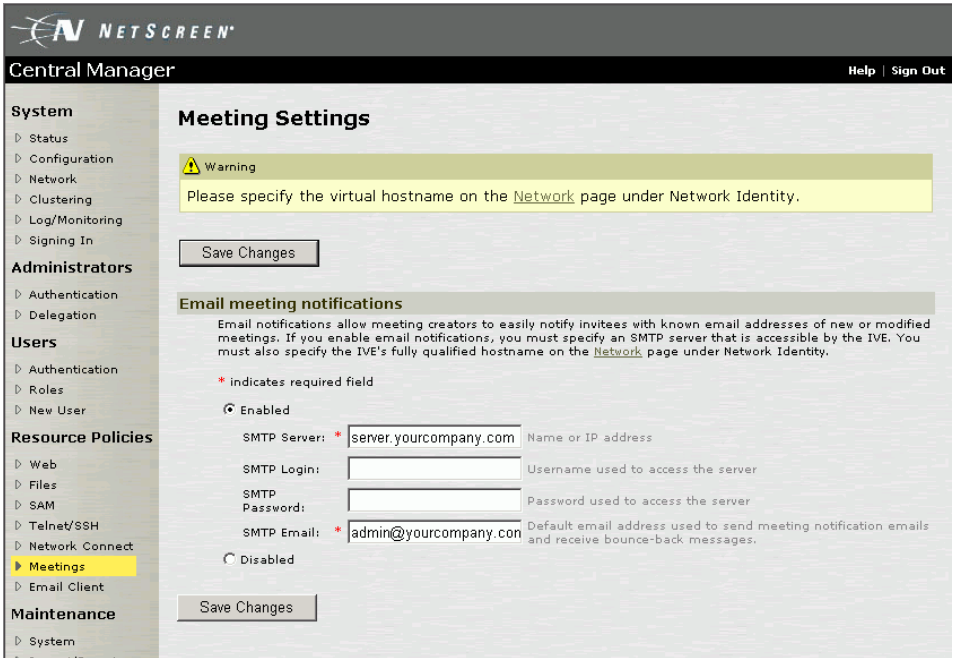


Abbildung 109:Resource Policies > Meetings

Konfigurieren der Seite „Email Client“

Auf der Seite **Resource Policies > E-Mail-Client** können Sie Folgendes durchführen:

Schreiben einer E-Mail-Client-Ressourcenrichtlinie für Mailserver 379

Durch die Aktualisierungsoption Secure Email Client können Remotebenutzer über einen Webbrowsers und eine Internetverbindung auf standardbasierte E-Mail-Anwendungen wie Outlook Express, Netscape Communicator oder Eudora von Qualcomm zugreifen. Weitere Informationen finden Sie unter „E-Mail-Client – Übersicht“ auf Seite 85.

Schreiben einer Ressourcenrichtlinie für E-Mail-Client

Wenn Sie die Zugriffsfunktion E-Mail-Client für eine Rolle aktivieren, müssen Sie eine Ressourcenrichtlinie erstellen, die Einstellungen für den Mailserver angibt. Im Gegensatz zu anderen Zugriffsfunktionen verfügt Secure Email Client nur über eine Ressourcenrichtlinie, die für *alle* Rollen gilt, für die diese Funktion aktiviert ist. Wenn Sie den E-Mail-Client-Dienst für Benutzer aktivieren, müssen Sie IMAP-, POP- und SMTP-Mailserverinformationen und Einstellungen für die Benutzerauthentifizierung angeben. Das IVE fungiert als E-Mail-Proxy für den bzw. die angegebenen Server.

Das IVE unterstützt mehrere Mailserver. Sie können festlegen, dass alle Benutzer einen Standardmailserver verwenden müssen, oder Sie können Benutzern die Möglichkeit geben, einen benutzerdefinierten SMTP- und IMAP- bzw. POP-Mailserver anzugeben. Wenn Sie Benutzern das Festlegen eines benutzerdefinierten Mailservers ermöglichen, müssen diese die Servereinstellungen über das IVE vornehmen. Der IVE-Server verwaltet die E-Mail-Benutzernamen, um Namenskonflikte zu vermeiden.

☑ Schreiben einer E-Mail-Client-Ressourcenrichtlinie für Mailserver

So schreiben Sie eine E-Mail-Client-Ressourcenrichtlinien für Mailserver:

1. Wählen Sie in der Web console **Resource Policies > E-Mail-Client** aus.
2. Klicken Sie unter **Email Client Support** auf **Enabled**.

3. Wählen Sie unter **Email Authentication Mode** eine der folgenden Optionen aus:
   - **Web-based email session**

     Benutzer müssen eine einmalige E-Mail-Einrichtung für das IVE vornehmen. Anschließend konfigurieren sie ihren E-Mail-Client so, dass der Benutzername und das Kennwort verwendet werden, die durch die E-Mail-Einrichtung für das IVE generiert werden. Es empfiehlt sich, dass die Benutzer sich an dem IVE anmelden, um eine E-Mail-Sitzung zu starten. (Standardeinstellung.)
   - **Combined IVE and mail server authentication**

     Benutzer konfigurieren ihren E-Mail-Client so, dass die folgenden Anmeldeinformationen verwendet werden:
     - Benutzername: Der normale Benutzername eines Benutzers für den Mailserver oder ein Benutzername, der beim E-Mail-Setup für das IVE generiert wird, wenn eine der folgenden Bedingungen zutrifft:
       - der Benutzer verfügt über mehrere Benutzernamen für den Mailserver
       - die Benutzernamen auf dem IVE-Server und dem Mailserver sind unterschiedlich
     - Kennwort: Das IVE-Kennwort des Benutzers, gefolgt von einem benutzerdefinierbaren Trennzeichen für Anmeldeinformationen, gefolgt von dem Mailserverkennwort des Benutzers.

     Benutzer müssen sich nicht am beim IVE anmelden, um E-Mail zu verwenden.
   - **Mail server authentication only**

     Benutzer konfigurieren ihren E-Mail-Client so, dass ihre normalen Mailserver-Benutzernamen und -Kennwörter verwendet werden. Benutzer müssen sich nicht am IVE anmelden, um E-Mail zu verwenden oder zu konfigurieren.

   Hinweis: Die Benutzer können ihre Benutzernamen und Kennwörter für E-Mail problemlos auf der Seite **Email Setup** ermitteln.

4. Geben Sie unter **Default Server Information** Ihre Mailserverdaten an. Das IVE fungiert als E-Mail-Proxy für diesen Server.

Wichtig: Sie können nur einen Standardmailserver angeben. Wenn Benutzer E-Mail-Nachrichten von mehreren SMTP- und POP- bzw. IMAP-Servern abrufen müssen, bieten Sie ihnen durch Aktivieren des entsprechenden Kontrollkästchens die Möglichkeit, weitere Mailserver zu definieren. Wenn Sie Benutzern die Festlegung benutzerdefinierter Server ermöglichen, müssen die Benutzer diese Informationen auf ihrer IVE-Seite „Email Setup“ eingeben.

5. Geben Sie unter **Email Session Information** Folgendes an:
   - Einen **Idle Timeout**-Wert, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.
   - Einen Wert für **Max. Session Length**, der angibt, wie lange sich die E-Mail-Sitzung eines Benutzers im Leerlauf befinden kann, bevor das IVE die E-Mail-Sitzung beendet.
6. Klicken Sie auf **Save Changes**.

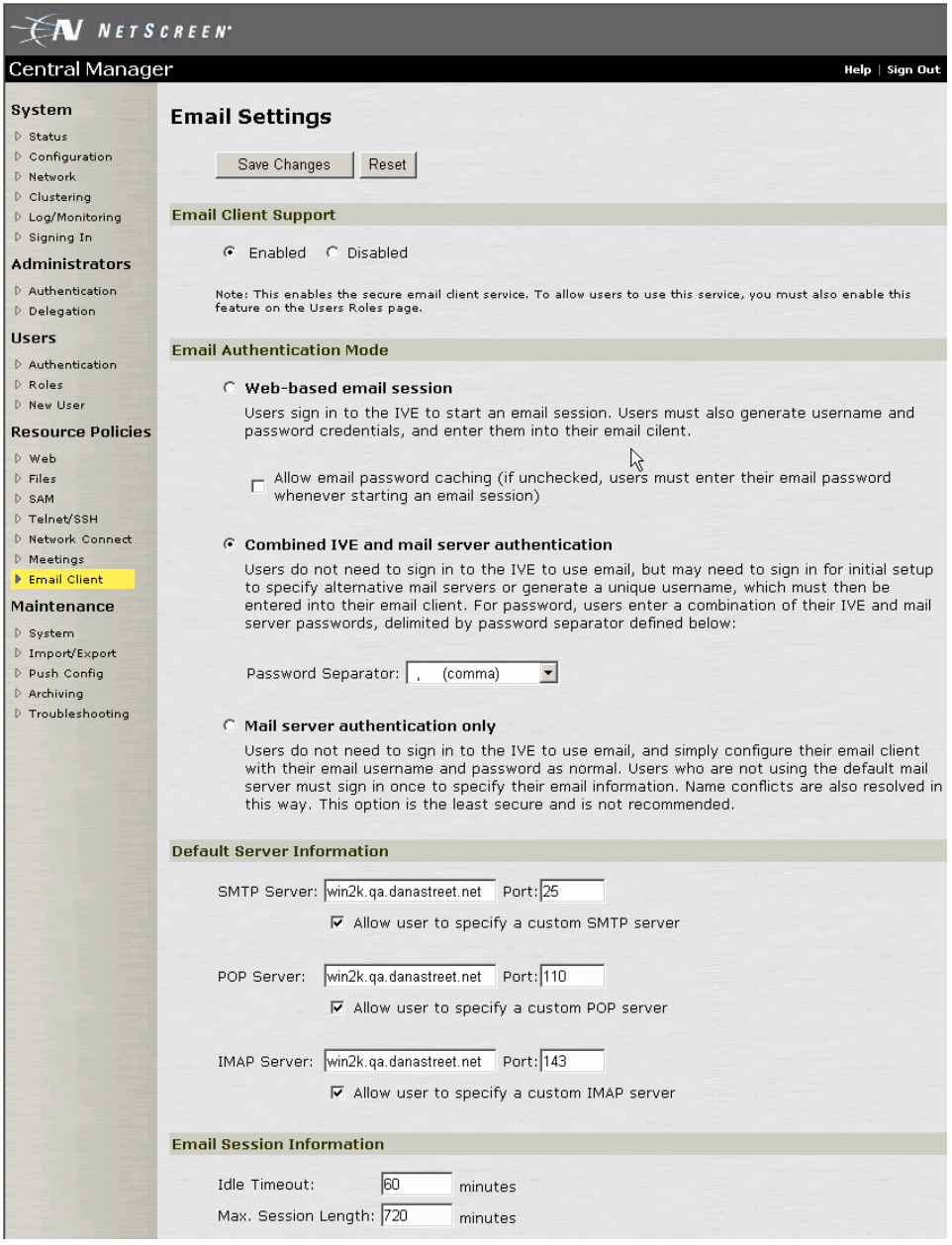

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Email Settings
Save Changes
Reset
Email Client Support
Enabled
Disabled
Note: This enables the secure email client service. To allow users to use this service, you must also enable this feature on the Users Roles page.
Email Authentication Mode
Web-based email session
Users sign in to the IVE to start an email session. Users must also generate username and password credentials, and enter them into their email cilent.
Allow email password caching (if unchecked, users must enter their email password whenever starting an email session)
Combined IVE and mail server authentication
Users do not need to sign in to the IVE to use email, but may need to sign in for initial setup to specify alternative mail servers or generate a unique username, which must then be entered into their email client. For password, users enter a combination of their IVE and mail server passwords, delimited by password separator defined below:
Password Separator: , (comma)
Mail server authentication only
Users do not need to sign in to the IVE to use email, and simply configure their email client with their email username and password as normal. Users who are not using the default mail server must sign in once to specify their email information. Name conflicts are also resolved in this way. This option is the least secure and is not recommended.
Default Server Information
SMTP Server: win2k.qa.danastreet.net Port: 25
Allow user to specify a custom SMTP server
POP Server: win2k.qa.danastreet.net Port: 110
Allow user to specify a custom POP server
IMAP Server: win2k.qa.danastreet.net Port: 143
Allow user to specify a custom IMAP server
Email Session Information
Idle Timeout: 60 minutes
Max. Session Length: 720 minutes

Abbildung 110:Resource Policies > Email Client

Konfigurieren der Seite „System“

Die Seite **Maintenance > System** enthält die folgenden Registerkarten:

Registerkarte „Platform“ 383
Registerkarte „Upgrade/Downgrade“ 384
Registerkarte „Options“ 386

Auf der Seite **Maintenance > System** können Sie Folgendes durchführen:

Neustarten, Herunterfahren und Testen der Verbindung 383
Installieren eines NetScreen-Softwaredienstpakets 385
Aktivieren von Versionsüberwachung und Beschleunigerkarten 386

Registerkarte „Platform“

☑ Neustarten, Herunterfahren und Testen der Verbindung

Auf der Seite **Platform** können Sie die IVE-Verbindung neu starten, herunterfahren oder testen sowie Systemdaten anzeigen (beispielsweise den IVE-Hostnamen und die Zeit des letzten Neustarts). Informationen zur Handhabung der folgenden Situationen finden Sie in „Anhang D: “ auf Seite 453:

- Sie haben Ihre Anmeldedaten vergessen.
- Sie haben die IP-Beschränkungen so eingestellt, dass Sie sich nicht mehr am Gerät anmelden können.
- Sie möchten das System in den vorherigen Zustand zurücksetzen.
- Sie müssen das System auf die Werkseinstellungen zurücksetzen.

So starten Sie die Serververbindung neu, fahren sie herunter oder testen sie:

1. Wählen Sie in der Web console **Maintenance > System > Platform** aus.
2. Klicken Sie auf **Reboot Now**, um das IVE neu zu starten.
3. Klicken Sie auf **Shutdown**, um das IVE herunterzufahren. Der Server wird heruntergefahren, und Sie müssen den Reset-Schalter an der Appliance drücken, um den Server neu zu starten. Beachten Sie, dass das Gerät nach dem Herunterfahren des Servers eingeschaltet bleibt.

4. Klicken Sie auf **Test Server Connectivity**, um einen ICMP-Ping-Befehl vom IVE an alle Server zu senden, die das IVE verwendet, und ihre Verbindung zu testen. Der Status der einzelnen Server wird unter **Server Connectivity Results** aufgeführt.

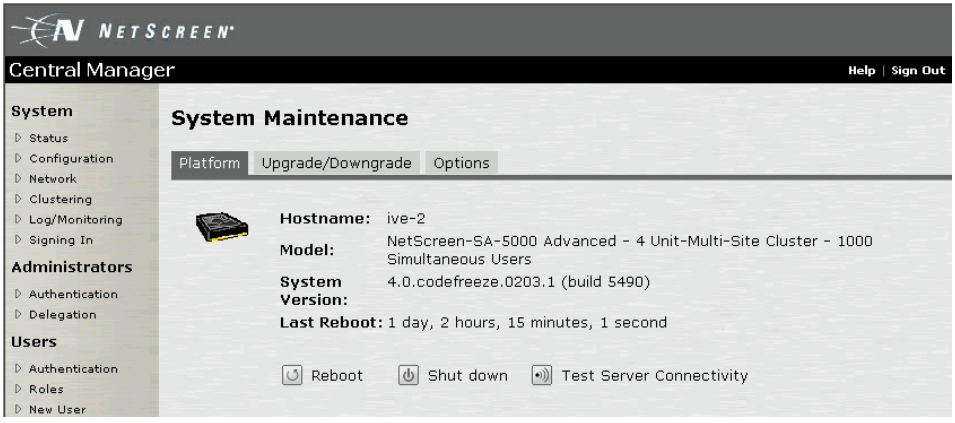


Abbildung 111:Maintenance > System > Platform

Registerkarte „Upgrade/Downgrade“

Sie installieren ein anderes Dienstpaket, indem Sie zuerst von der NetScreen Support-Website die Software herunterladen und diese dann über die Web console hochladen. Paketdateien werden verschlüsselt und signiert, sodass der IVE-Server nur gültige, von NetScreen ausgegebene Pakete akzeptiert. Mit dieser Maßnahme wird verhindert, dass der IVE-Server als „Trojanische Pferde“ bezeichnete Programme akzeptiert.

Dieses Feature wird meist dazu verwendet, Aktualisierungen auf neuere Versionen der Systemsoftware durchzuführen. Sie können jedoch mit diesem Verfahren die Systemsoftware auch auf eine ältere Version herunterstufen oder alle aktuellen Konfigurationseinstellungen löschen und eine neue Ausgangsbasis schaffen. Ein Rollback zu einem vorherigen Systemzustand ist auch über die serielle Konsole möglich. Dieser Vorgang ist unter „Rollback zu einem vorherigen Systemzustand“ auf Seite 454 beschrieben.

Hinweis: Die Installation eines neuen Dienstpakets kann einige Minuten dauern. Das IVE muss anschließend neu gestartet werden. Da bei diesem Vorgang die vorhandenen Systemdaten gesichert werden, lässt sich die Installationsdauer verkürzen, indem der Inhalt des Systemprotokolls vor der Installation eines Dienstpakets gelöscht wird.

☑ Installieren eines NetScreen-Softwaredienstpakets

Exportieren Sie vor der Installation eines neuen Dienstpakets die aktuelle Systemkonfiguration, die lokalen Benutzerkonten, die Lesezeichen der Benutzer und die Rollen- und Richtlinieninformationen, wie unter „Konfigurieren der Seite „Import/Export"" auf Seite 389 erläutert.

So installieren Sie ein Dienstpaket:

1. Navigieren Sie zur NetScreen Support-Website „http://support.netscreen.com", und rufen Sie das gewünschte Dienstpaket ab.
2. Wählen Sie in der Web console **Maintenance >System > Upgrade/Downgrade**. aus.
3. Klicken Sie auf **Browse**, um das von der Supportsite heruntergeladene Dienstpaket auf der Festplatte zu suchen. Wenn Sie die aktuellen Konfigurationseinstellungen löschen, aber weiterhin dieselbe IVE-Version verwenden möchten, wählen Sie das derzeit in Ihrer Appliance installierte Dienstpaket aus.
4. Wenn Sie die Software auf ein älteres Dienstpaket herunterstufen oder die Konfigurationseinstellungen löschen, wählen Sie **Delete all system and user data**.

Wichtig: Wenn Sie das IVE zurücksetzen und mit dieser Option alle System- und Benutzerdaten aus der Appliance löschen möchten, müssen Sie vor der erneuten Systemkonfiguration die Netzwerkverbindungen wiederherstellen. Beachten Sie außerdem, dass kein Rollback auf eine ältere IVE-Version als 3.1 durchgeführt werden kann.

---

5. Wählen Sie die Dienstpaketdatei aus, und klicken Sie auf **Install Now**.

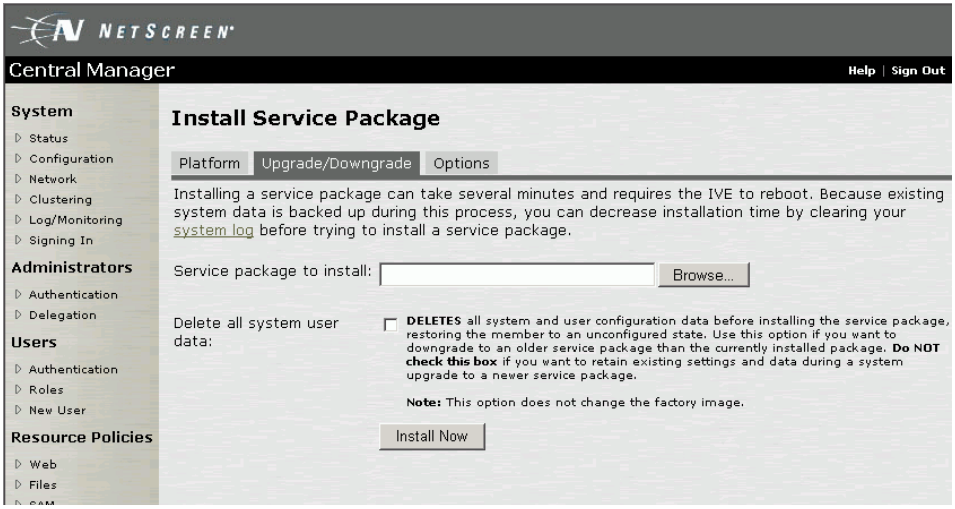

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
Install Service Package
Platform
Upgrade/Downgrade
Options
Installing a service package can take several minutes and requires the IVE to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system log before trying to install a service package.
Service package to install:
Browse...
Delete all system user data:
DELETES all system and user configuration data before installing the service package, restoring the member to an unconfigured state. Use this option if you want to downgrade to an older service package than the currently installed package. Do NOT check this box if you want to retain existing settings and data during a system upgrade to a newer service package.
Note: This option does not change the factory image.
Install Now

Abbildung 112:Maintenance > System > Upgrade/Downgrade

Registerkarte „Options“

☑ Aktivieren von Versionsüberwachung und Beschleunigerkarten

Damit das System auf dem neuesten Stand und sicher bleibt, können Sie sich vom IVE automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigen lassen. Hierzu werden die folgenden Daten an NetScreen gemeldet: Name Ihrer Firma, MD5-Hash Ihrer Lizenzeinstellungen und Informationen zur aktuellen Softwareversion. Auf der Seite **Options** können außerdem Beschleunigerkarten zur Leistungssteigerung aktiviert werden.

Hinweis: Die Einstellungen für die Beschleunigerkarte werden nur angezeigt, wenn Sie ein A5000-IVE mit der entsprechenden Karte erworben haben.

So aktivieren Sie automatische Aktualisierungen und Beschleunigerkarten:

1. Wählen Sie in der Web console **Maintenance > System > Options** aus.

2. Aktivieren Sie das Kontrollkästchen **Automatic Version Monitoring**, um automatisch über wichtige Softwarepatches und -aktualisierungen benachrichtigt zu werden.

   Wichtig: Zum Schutz Ihres Systems wird dringend empfohlen, diesen automatischen Dienst zu aktivieren. Sie können ihn jedoch ggf. auch deaktivieren.

3. Aktivieren Sie das Kontrollkästchen **SSL Accelerator**, damit die Ver- und Entschlüsselung von SSL-Handshakes von der Appliance an die Beschleunigerkarte delegiert wird (optional).
4. Aktivieren Sie das Kontrollkästchen **ZIP Accelerator**, damit alle HTML-, JavaScript- und CSS-Daten komprimiert werden, auf die beim Webbrowsing oder bei der Dateinavigation zugegriffen wird (optional).
5. Klicken Sie auf **Save Changes**.

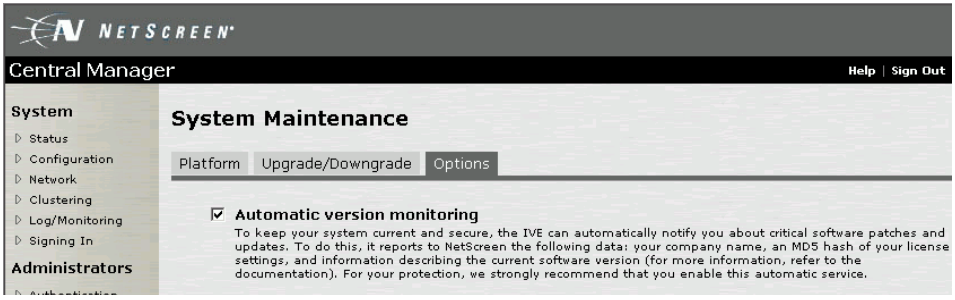

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
System Maintenance
Platform
Upgrade/Downgrade
Options
Automatic version monitoring
To keep your system current and secure, the IVE can automatically notify you about critical software patches and updates. To do this, it reports to NetScreen the following data: your company name, an MD5 hash of your license settings, and information describing the current software version (for more information, refer to the documentation). For your protection, we strongly recommend that you enable this automatic service.

Abbildung 113:Maintenance > System > Options

Konfigurieren der Seite „Import/Export“

Die Seite **Maintenance > Import/Export** enthält die folgenden Registerkarten:

Registerkarte „Configuration“ 389
Registerkarte „User Accounts“ 393
Registerkarte „Roles and Policies“ 394

Auf der Seite **Maintenance > Import/Export** können Sie Folgendes durchführen:

Exportieren einer Systemkonfigurationsdatei 389
Importieren einer Systemkonfigurationsdatei 390
Exportieren lokaler Benutzerkonten 393
Importieren lokaler Benutzerkonten 393
Exportieren von Rollen und Ressourcenrichtlinien 395
Importieren von Rollen und Ressourcenrichtlinien 397

Registerkarte „Configuration“

Mithilfe dieser Registerkarte können Sie eine Systemkonfigurationsdatei importieren oder exportieren. Die Systemkonfigurationsdatei enthält alle System- und Netzwerkeinstellungen. Weitere Informationen zum Festlegen eines Archivierungsplans für die Serverkonfiguration finden Sie unter „Planen der Archivierung von Systemdaten auf einem externen FTP-Server“ auf Seite 403.

☑ Exportieren einer Systemkonfigurationsdatei

Exportieren einer Systemkonfigurationsdatei:

1. Wählen Sie in der Web console **System > Import/Export > Configuration** aus.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.

3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

Wichtig: Beim Exportieren einer Access Series FIPS-Konfigurationsdatei müssen Sie beachten, dass in dieser Datei auch Informationen über die Security World des Geräts enthalten sind. Daher benötigen Sie eine Administratorkarte, die der Security World zugeordnet ist, um die Konfigurationsdatei auf ein anderes Gerät importieren zu können.

☑ Importieren einer Systemkonfigurationsdatei

Beim Importieren einer Systemkonfigurationsdatei können Sie das Serverzertifikat und die IP-Adresse oder die Netzwerkeinstellungen des IVE-Servers aus den importierten Informationen ausschließen. Um beispielsweise mehrere IVEs hinter einem Load-Balancer einzurichten, importieren Sie alle Daten außer der IP-Adresse. Um ein IVE als Sicherungsserver einzurichten, importieren Sie alle Daten außer dem digitalen Zertifikat und den Netzwerkeinstellungen.

Hinweis: Beim Importieren einer Konfigurationsdatei mit Lizenzen erhalten im IVE die bestehenden Lizenzen Vorrang, die gegenwärtig auf dem IVE installiert sind. Archivierte Lizenzen werden nur importiert, wenn auf dem IVE gegenwärtig keine Lizenzen vorhanden sind.

So importieren Sie eine Konfigurationsdatei:

1. Wählen Sie in der Web console **System > Import/Export > Configuration** aus.
2. Geben Sie an, ob Sie das Serverzertifikat importieren möchten. Das Zertifikat wird nur importiert, wenn Sie das Kontrollkästchen **Import Server Certificate?** aktivieren.

Wichtig: Beim Importieren eines Serverzertifikats auf ein Access Series FIPS-System müssen Sie ein Zertifikat auswählen, bei dem ein FIPS-kompatibler privater Schlüssel verwendet wird. Um FIPS-Kompatibilität zu gewährleisten, wählen Sie ein Zertifikat und die zugehörigen privaten Security World-Schlüssel aus, die auf einem Access Series FIPS-System erzeugt wurden.

---

3. Wählen Sie eine Importoption aus. Beachten Sie folgende Punkte:
   - Wenn Sie die IP-Adresse ausschließen, wird die IP-Adresse des Servers beim Importieren der Datei nicht geändert.
   - Wenn Sie die Netzwerkeinstellungen ausschließen, werden die Informationen auf der Seite **System > Network Settings** (Einstellungen für internen Port, externen Port und statische Routen) beim Importieren der Datei nicht geändert.
4. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `system.cfg` heißt.
5. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
6. Klicken Sie auf **Import Config**.

Wichtig: Beim Importieren eines Serverzertifikats und der zugehörigen Security World auf ein Access Series FIPS-Gerät, müssen Sie die Initialisierung der Security World mit der seriellen Konsole und mit einer Administratorkarte abschließen, die der neuen, importierten Security World zugeordnet ist. Weitere Informationen finden Sie unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 463.

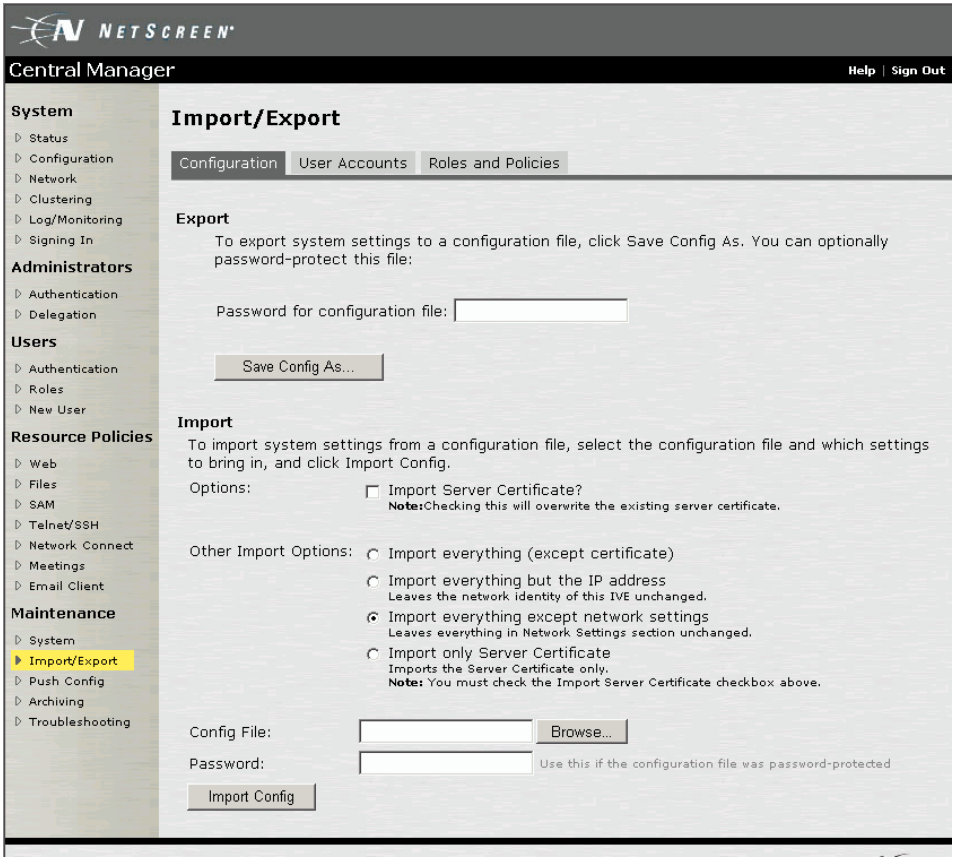


Abbildung 114:Maintenance > Import/Export > Configuration

Registerkarte „User Accounts“

Mithilfe dieser Registerkarte können Sie lokale Benutzerkonten importieren oder exportieren. In der Benutzerkontendatei sind sämtliche lokalen Benutzer enthalten, die Sie für alle lokalen Authentifizierungsserver definiert haben. Weitere Informationen zum Festlegen eines Archivierungsplans für Benutzerdatensätze finden Sie unter „Planen der Archivierung von Systemdaten auf einem externen FTP-Server“ auf Seite 403.

☑ Exportieren lokaler Benutzerkonten

Exportieren einer Systemkonfigurationsdatei:

1. Wählen Sie in der Web console **System > Import/Export > Configuration** aus.
2. Geben Sie unter **Export** ein Kennwort ein, wenn die Konfigurationsdatei durch ein Kennwort geschützt werden soll.
3. Klicken Sie zum Speichern der Datei auf **Save Config As**.

☑ Importieren lokaler Benutzerkonten

So importieren Sie lokale Benutzerkonten:

1. Wählen Sie in der Administratorkonsole Web console **System > Import/Export >User Accounts** aus.
2. Wechseln Sie zu der Konfigurationsdatei, die in der Standardeinstellung `user.cfg` heißt.
3. Geben Sie das für die Datei festgelegte Kennwort ein. Wenn Sie vor dem Export der Datei kein Kennwort festgelegt haben, lassen Sie dieses Feld leer.
4. Klicken Sie auf **Import Config**.

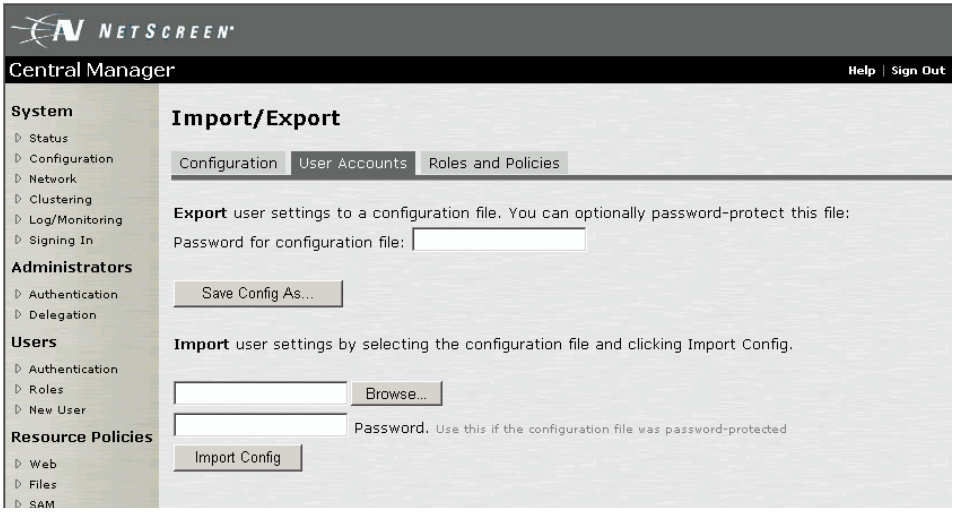


Abbildung 115:Maintenance > Import/Export > User Accounts

Registerkarte „Roles and Policies“

Die Seite **Maintenance > Import/Export > Roles and Resources** ermöglicht das Exportieren ausgewählter delegierter Administrationsrollen, Benutzerrollen und Ressourcenrichtlinien auf ein IVE und das anschließende Reimportieren auf ein anderes IVE. (Zum Kopieren von Rollen und Ressourcenrichtlinien aus einem IVE auf ein anderes können Sie auch die Konfigurationsübertragung (Seite 399) verwenden.)

Wichtig: Es wird nicht empfohlen, eine XML-Datei vor dem Importieren auf ein IVE zu verändern. Dies kann Konfigurationsfehler verursachen, die schwer aufzuspüren und zu beheben sind.

☑ Exportieren von Rollen und Ressourcenrichtlinien

So exportieren Sie Rollen und Ressourcenrichtlinien:

1. Wählen Sie in der Web console **Maintenance > Import/Export > Roles and Policies> Export** aus.
2. Aktivieren Sie das Kontrollkästchen **Delegated Admin Roles**, um delegierte Administrationsrollen zu kopieren. Gehen Sie anschließend folgendermaßen vor:
   - Wählen Sie **All roles** aus, um alle delegierten Administrationsrollen zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen kopieren möchten.
3. Aktivieren Sie das Kontrollkästchen **User Roles**, um Benutzerrollen zu kopieren.
   - Wählen Sie **All roles** aus, um alle delegierten Administratorrollen zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen kopieren möchten.
4. Aktivieren Sie das Kontrollkästchen **Resource Policies** , um Ressourcenrichtlinien zu kopieren. Aktivieren Sie anschließend die Kontrollkästchen für die Typen von Ressourcenrichtlinien, die Sie kopieren möchten, beispielsweise Richtlinien für Zugriffssteuerung, Zwischenspeicherung oder selektives Neuschreiben.
5. Klicken Sie auf **Export Configuration** , um die Informationen in einer XML-Datei zu speichern.

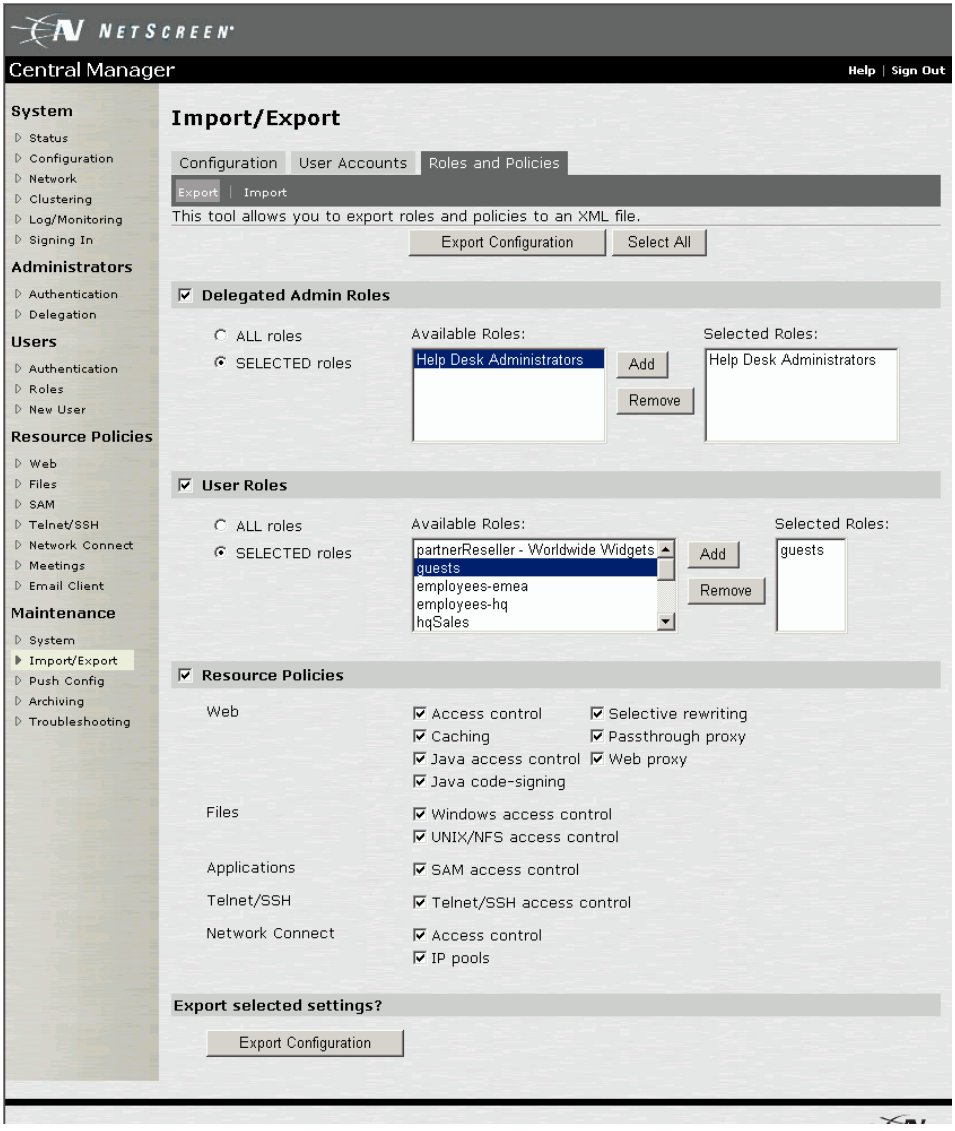


Abbildung 116:Maintenance > Import/Export > Roles and Policies > Export

☑ Importieren von Rollen und Ressourcenrichtlinien

So importieren Sie Rollen und Ressourcenrichtlinien:

1. Wählen Sie in der Web console **Maintenance > Import/Export > Roles and Policies> Import** aus.
2. Navigieren Sie zu dem Verzeichnis mit der XML-Datendatei, die Sie importieren möchten.
3. Aktivieren Sie das Kontrollkästchen **Overwrite duplicate settings**, um die Einstellungen auf dem Ziel-IVE mit Einstellungen zu überschreiben (nicht anzuhängen), die in der XML-Datei enthalten sind (optional).
4. Klicken Sie auf **Import Settings**.

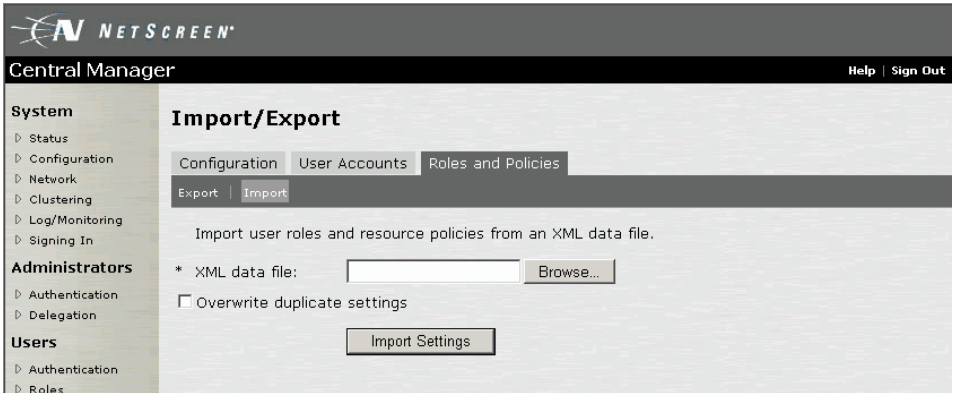


Abbildung 117:Maintenance > Import/Export > Roles and Policies > Import

Konfigurieren der Seite „Push Config“

☑ Kopieren von Rollen und Ressourcenrichtlinien zwischen IVEs

Auf der Seite **Maintenance > Push Config** können ausgewählte delegierte Administrationsrollen, Benutzerrollen und Ressourcenrichtlinien über Konfigurationsübertragung von einem IVE auf ein anderes IVE übertragen werden. Diese Funktion ermöglicht eine einfache Konfigurationsverwaltung für das gesamte Unternehmen, ohne dass IVE-Appliances in Cluster aufgeteilt werden müssen. Mithilfe der Konfigurationsübertragung können Sie gezielt entscheiden, welche delegierten Administrationsrollen, Benutzerrollen und Typen von Ressourcenrichtlinien unternehmensweit kopiert werden sollen. Beachten Sie, dass die Konfigurationsübertragung nur mit dem Central Manager-Paket verfügbar ist (Seite 67).

Um eine Konfiguration zu übertragen, müssen Sie Administratorkonten auf beiden IVEs erstellen. Die Konfigurationsübertragungs-Funktion meldet sich dann anhand der Administratorinformationen automatisch auf dem Ziel-IVE an. Beachten Sie beim Erstellen eines Administratorkontos Folgendes:

- Sie müssen der **.Administrators**-Rolle zugeordnet sein, d.h. einen „Superadministrator“ mit vollen Administratorberechtigungen erstellen.
- Das Zieladministratorkonto für das IVE muss Authentifizierung mit statischen Kennwörtern oder 2-Faktor-Tokens verwenden, die keine Authentifizierung vom Typ Challenge-Response verwenden. (Zertifikate, Soft ID und Defender-Authentifizierung werden z.B. nicht unterstützt.)
- Sie dürfen das Administratorkonto nicht so konfigurieren, dass der Administrator eine Rolle auswählen muss, um sich auf dem Ziel-IVE anzumelden. (Sie dürfen einen einzelnen Benutzer z.B. nicht mehreren Rollen zuordnen, auch nicht der Rolle des Konfigurationsübertragung-Administrators, sofern Sie diese Rollen nicht permissiv zusammenführen.) Wir empfehlen das Erstellen eines Kontos, das ausschließlich Administratoren für die Konfigurationsübertragung vorbehalten ist. Dies gewährleistet, dass der Administrator bei der Anmeldung keine Rolle auswählen muss und die Aktionen von Administratoren für die Konfigurationsübertragung in den Protokolldateien eindeutig nachvollzogen werden können.

So übertragen Sie ausgewählte Rollen und Ressourcen von einem IVE auf ein anderes:

1. Erstellen von Administratorkonten auf beiden IVE-Appliances. Anweisungen hierfür finden Sie unter „Konfigurieren der Seite „Delegation"" auf Seite 265. (Siehe die oben aufgeführten Beschränkungen.)
2. Wählen Sie in der Web console **Maintenance > Push Config** aus.
3. Geben Sie unter **Target Host Sign-in URL** den Administrator-URL des IVE ein, auf den Rollen und Ressourcenrichtlinien übertragen werden sollen. Beispiel: https://10.10.10.10/admin.
4. Geben Sie den Benutzernamen, das Kennwort und den Authentifizierungsbereich eines Administratorkontos auf dem Ziel-IVE ein, das über volle Administratorberechtigungen verfügt.
5. Aktivieren Sie das Kontrollkästchen **Overwrite duplicate settings**, wenn Sie Benutzerrollen, delegierte Administrationsrollen und Ressourcenrichtlinien auf dem Ziel-IVE überschreiben wollen, die den gleichen Namen wie eine Benutzerrolle, delegierte Administrationsrolle oder Ressourcenrichtlinie auf dem Quell-IVE aufweisen.
6. Aktivieren Sie das Kontrollkästchen **Delegated Admin Roles**, um delegierte Administrationsrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **All roles** aus, um alle delegierten Administrationsrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen auf das Ziel-IVE kopieren möchten.
7. Aktivieren Sie das Kontrollkästchen **User Roles**, um Benutzerrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **All roles** aus, um alle delegierten Administratorrollen auf das Ziel-IVE zu kopieren.
   - Wählen Sie **Selected roles** und dann Rollen aus der Liste **Available Roles** aus. Klicken Sie auf **Add**, wenn Sie nur einige Rollen auf das Ziel-IVE kopieren möchten.
8. Aktivieren Sie das Kontrollkästchen **Resource Policies** , um Ressourcenrichtlinien auf das Ziel-IVE zu kopieren. Aktivieren Sie anschließend die Kontrollkästchen für die Typen von Ressourcenrichtlinien, die Sie kopieren möchten, beispielsweise Richtlinien für Zugriffssteuerung, Zwischenspeicherung oder selektives Neuschreiben.
9. Klicken Sie auf **Push Configuration**, um die ausgewählten Rollen und Ressourcen auf das Ziel-IVE zu kopieren. Das IVE zeigt den Übertragungsstatus unten auf der Seite **Maintenance > Push Config** im Quell-IVE an.

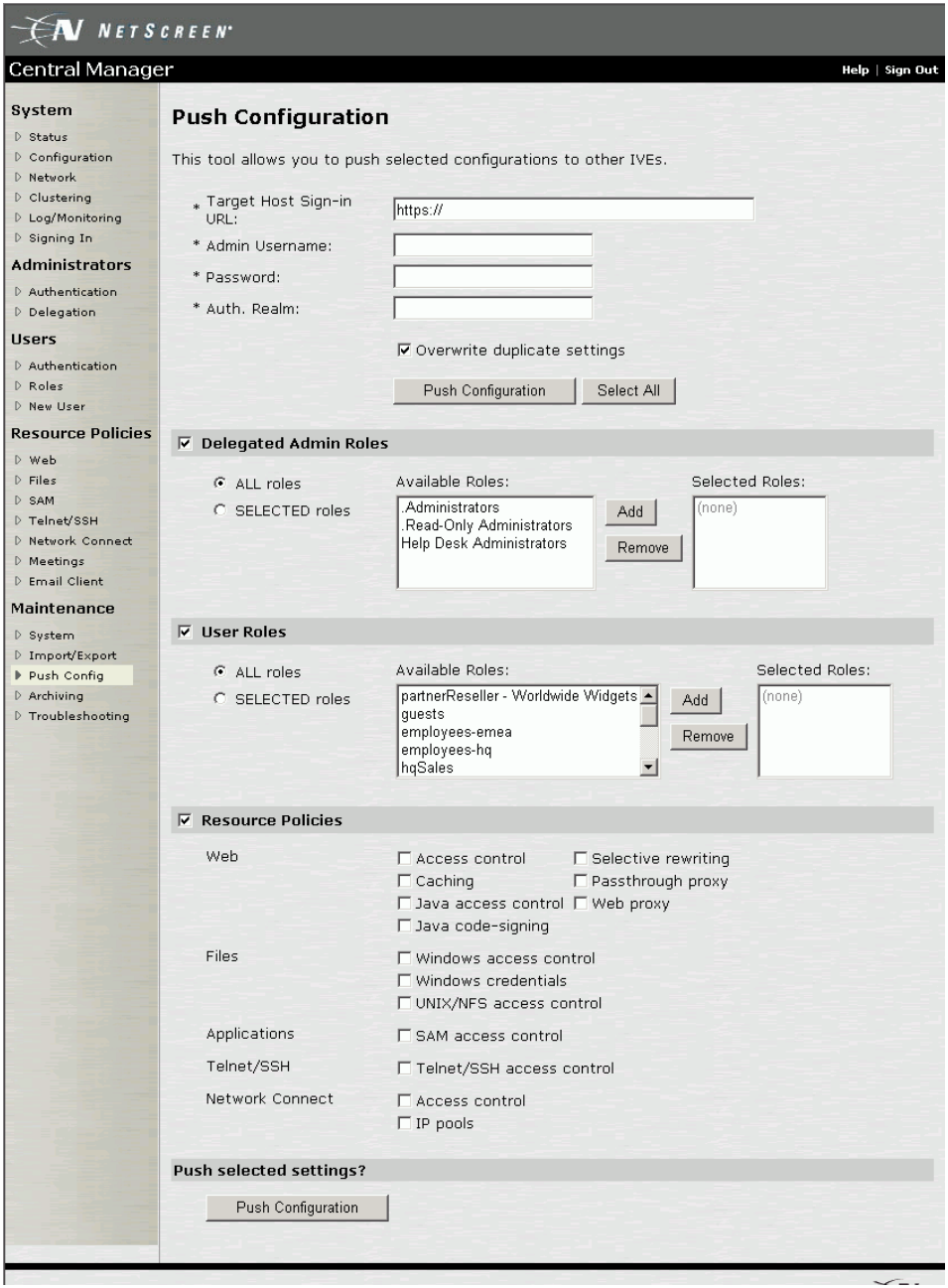


Abbildung 118:Maintenance > Push Config

Konfigurieren der Seite „Archiving“

Die Seite **Maintenance > Archiving** enthält die folgenden Registerkarten:

Registerkarte „FTP Server“ 403
Registerkarte „Local Backups“ 406

Auf der Seite **Maintenance > Archiving** können Sie Folgendes durchführen:

Planen der Archivierung von Systemdaten auf einem externen FTP-Server 403
Speichern eines Snapshots der aktuellen Konfiguration 406
Wiederherstellen des System- oder Benutzerkontenstatus aus einem Snapshot 406

Registerkarte „FTP Server“

☑ Planen der Archivierung von Systemdaten auf einem externen FTP-Server

Sie können festlegen, dass Systemprotokolldateien, Konfigurationsdateien und Benutzerkonten täglich oder wöchentlich archiviert werden. Das IVE archiviert die Dateien an den von Ihnen ausgewählten Tagen und Uhrzeiten über FTP auf dem angegebenen Server und im angegebenen Verzeichnis. Die Konfigurationsdateien und Benutzerkonten werden verschlüsselt, um eine sichere Übertragung über FTP und eine sichere Speicherung auf anderen Servern zu gewährleisten.

Der Name der Archivdateien enthält, wie nachfolgend dargestellt, das Datum und die Uhrzeit der Archivierung:

- Systemkonfigurationsdateien: `NetScreenConf-`*`Datum-Uhrzeit`*
- Benutzerkonten: `NetScreenUserAccounts-`*`Datum-Uhrzeit`*
- Systemereignisse: `NetScreenccessLog-`*`Datum-Uhrzeit`*
- Administratorereignisse: `NetScreenAdminLog-`*`Datum-Uhrzeit`*
- Benutzereignisse: `NetScreenEventsLog-`*`Datum-Uhrzeit`*

So geben Sie Archivierungsparameter an:

1. Wählen Sie in der Web console **Maintenance > Archiving > FTP Server** aus.
2. Geben Sie unter **Archive Settings** den Zielserver, ein Verzeichnis und Ihre FTP-Anmeldeinformationen für diesen Server an. Schließen Sie keine Laufwerksangabe für das Zielverzeichnis ein, beispielsweise: `netscreen/log`.
   - Bei UNIX-Computern geben Sie abhängig vom Basisverzeichnis des Benutzers entweder einen absoluten oder einen relativen Pfad an.
   - Bei Windows-Computern geben Sie einen Pfad an, der relativ zum Ordner `ftproot` ist.
3. Geben Sie für alle Arten von archivierten Daten Sie einen Archivierungsplan an. Für Systemereignisse, Zugriff und Administratorprotokolle können Sie außerdem einen Protokollfilter angeben und den Inhalt der Protokolldatei nach der Archivierung löschen.
4. Klicken Sie auf **Save Changes**.

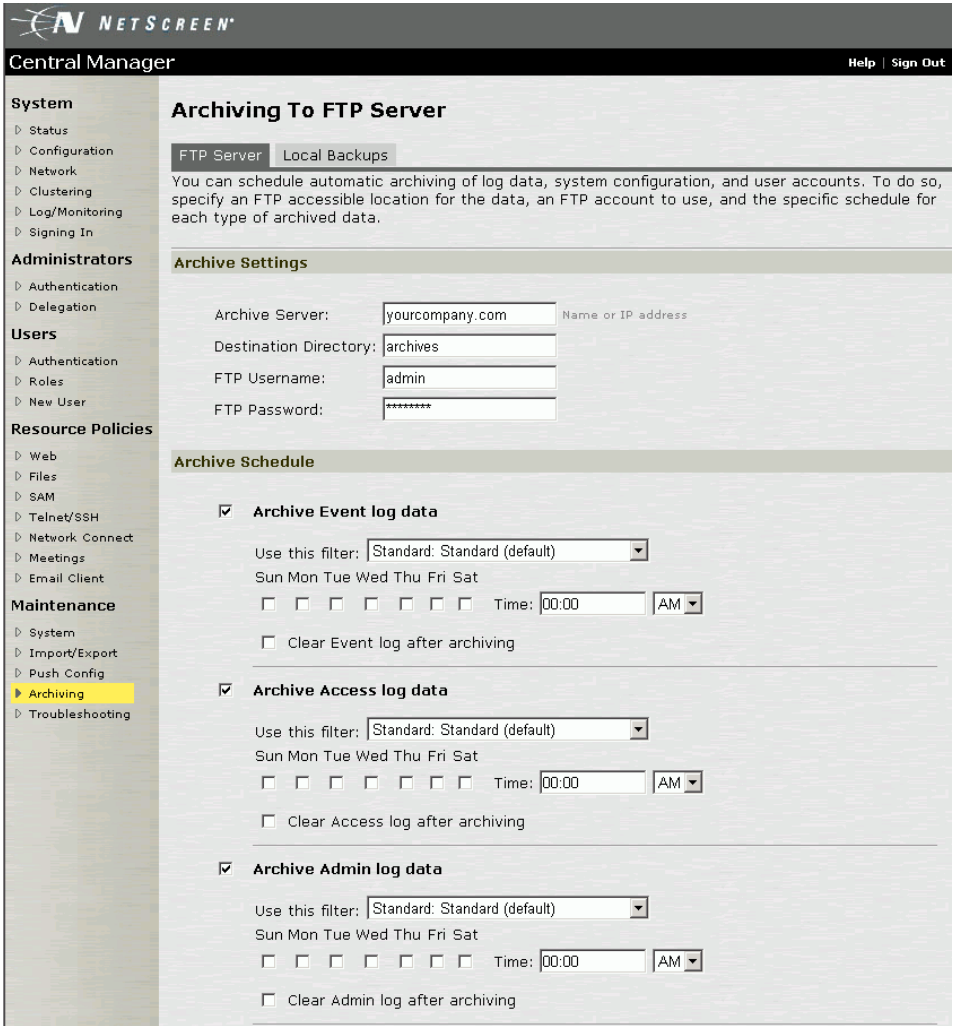


Abbildung 119:Maintenance > Archiving > FTP Server

Registerkarte „Local Backups“

☑ Speichern eines Snapshots der aktuellen Konfiguration

Mit den Central Manager-Appliances für Access Series und Meeting Series können Snapshots der aktuellen Systemkonfiguration und Benutzerkonten direkt im IVE gespeichert werden. Mithilfe dieser Konfigurationen können das IVE oder IVE-Cluster in dem Zustand wiederhergestellt werden, der in der verschlüsselten Datei enthalten ist. Beachten Sie, dass diese Dateien nur Konfigurationsinformationen und keine Protokolle enthalten.

Sie können auf dem IVE bis zu fünf Snapshots der Systemkonfiguration sowie fünf Snapshots von Benutzerkonten speichern. Wenn Sie diese Zahl überschreiten, überschreibt das IVE den ältesten Snapshot mit dem neuen Snapshot. Wenn der älteste Snapshot nicht überschrieben werden soll, müssen Sie vor dem Speichern des neuesten Snapshots einen anderen Snapshot auswählen, der gelöscht werden soll.

So speichern Sie die aktuelle Systemkonfiguration:

1. Wählen Sie in der Web console **Maintenance > Archiving > Local Backups** aus.
2. Klicken Sie auf **Save Configuration** oder **Save User Accounts**. Das IVE fügt der Liste einen neuen Snapshot hinzu und benennt ihn mit dem aktuellen Datum und der aktuellen Uhrzeit.

☑ Wiederherstellen des System- oder Benutzerkontenstatus aus einem Snapshot

System- und Benutzersnapshots können verwendet werden, um ein einzelnes IVE oder ein IVE-Cluster zu aktualisieren. Wenn Sie ein IVE wiederherstellen möchten, das Teil eines Clusters ist, überträgt das IVE die Konfiguration automatisch auf alle anderen Clustermitglieder. Das Cluster bleibt solange deaktiviert, bis die Einstellungen aller Clustermitglieder mithilfe der Snapshotkonfiguration aktualisiert wurden. Starten Sie das Cluster dann neu, und aktivieren Sie es.

So überschreiben Sie die Konfiguration mit Einstellungen aus einer Sicherungsdatei:

1. Wählen Sie in der Web console **Maintenance > Archiving > Local Backups** aus.
2. Aktivieren Sie das Kontrollkästchen neben der Sicherungsdatei für die Systemkonfiguration das Benutzerkonto, die zum Wiederherstellen des Systems verwendet werden soll.
3. Wenn Sie eine Systemkonfiguration wiederherstellen, müssen Sie angeben, ob dabei auch das Zertifikat, die IP-Adresse und die Netzwerkeinstellungen aus der Konfigurationsdatei übernommen werden sollen. Beachten Sie bei der Aktualisierung Folgendes:
   - **Access Series FIPS-System** – Wenn Sie ein Zertifikat importieren möchten, müssen Sie ein Zertifikat mit einem FIPS-kompatiblen privaten Schlüssel auswählen. Um FIPS-Kompatibilität zu gewährleisten, wählen Sie ein Zertifikat und die zugehörigen privaten Security World-Schlüssel aus, die auf einem Access Series FIPS-System erzeugt wurden.
   - **Gesamter Cluster** – Gehen Sie beim Einschließen von Netzwerkeinstellungen vorsichtig vor. Da IP-Adressen und andere Einstellungen wahrscheinlich nicht für alle Mitglieder des Clusters gelten, könnte die Kommunikation zwischen den Mitgliedern unterbrochen werden, nachdem die Einstellungen auf alle Mitglieder übertragen wurden.
4. Klicken Sie auf **Restore**. Die Änderungen werden erst nach einem Neustart des IVE wirksam. Anschließend müssen Sie sich erneut am IVE anmelden, um auf die Web console zugreifen zu können.

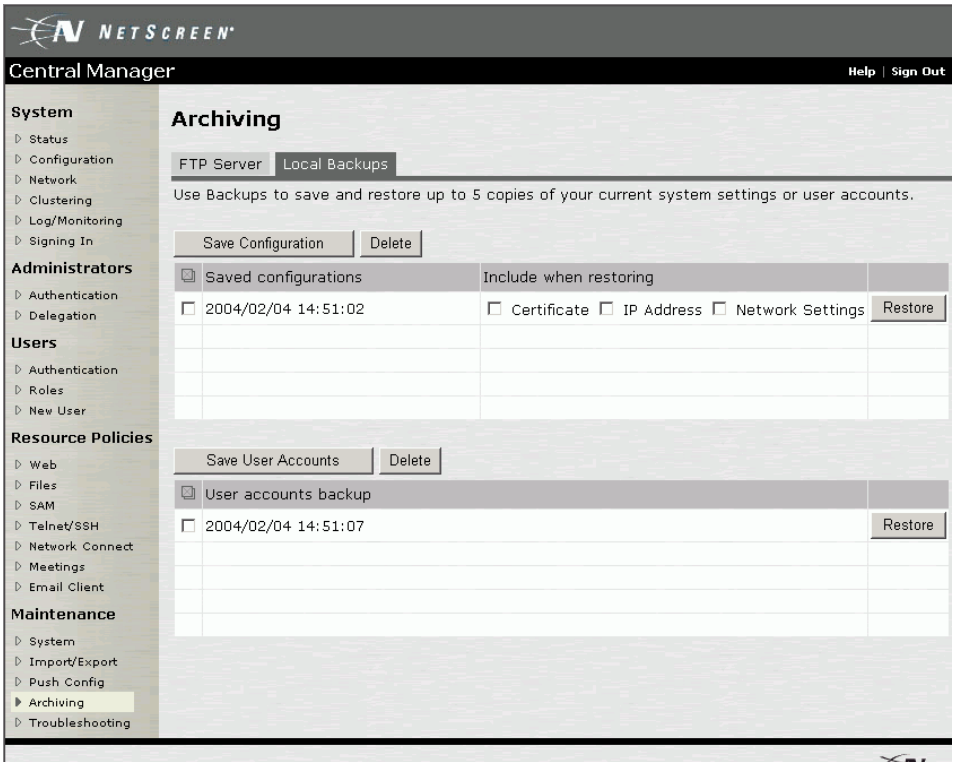


Abbildung 120:Maintenance > Archiving > Local Backups

Konfigurieren der Seite „Troubleshooting“

Die Seite **Maintenance >Troubleshooting** enthält die folgenden Registerkarten:

Registerkarte „Policy Tracing“ 409
Registerkarte „Session Recording“ 413
Registerkarte „System Snapshot“ 414
Registerkarte „TCP Dump“....415
Registerkarte „Commands“ 417
Registerkarte „Remote Debugging“....418

Auf der Seite **Maintenance > Troubleshooting** können Sie Folgendes durchführen:

Aufzeichnen einer Richtlinienverfolgungsdatei zur Fehlerbehebung 409
Aufzeichnen einer Ablaufverfolgungsdatei zur Fehlerbehebung....413
Erstellen eines Snapshots des IVE-Systemstatus 414
Sniffing von Netzwerkpaketheadern....415
Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls....417
Aktivieren von Remotefehlerbehebung für den NetScreen Support 418

Registerkarte „Policy Tracing“

☑ Aufzeichnen einer Richtlinienverfolgungsdatei zur Fehlerbehebung

Verwenden Sie diese Registerkarte, wenn Benutzer melden, dass Funktionen nicht wie erwartet verwendet werden können. Die Richtlinienverfolgung ermöglicht die Verfolgung einzelner Benutzer in jedem Bereich. Wenn Sie eine Richtlinienverfolgungsdatei für einen einzelnen Benutzer ausführen, zeigt das IVE Protokolleinträge an, in denen die Aktionen des Benutzers sowie Erklärungen aufgeführt sind, warum ihm der Zugriff auf verschiedene Rollen gewährt oder verweigert wird.

Sie können beispielsweise einen Bereich „Human Resources“ (Personalabteilung) mit zwei Rollenzuordnungsregeln erstellen:

- **All Employees**

  In dieser Rolle aktivieren Sie nur Webbrowsing. Benutzer werden mithilfe der folgenden Regel zugeordnet: if username = *, map to „All Employees“. (Jeder Benutzer, der sich in diesem Bereich anmelden darf, wird also automatisch der Rolle „All Employees“ zugeordnet.)

- **Human Resources Staff**

  Für diese Rolle aktivieren Sie die Web-, Datei- und Konferenzfunktionen. Benutzer werden mithilfe der folgenden Regel zugeordnet: if LDAP group=human resources, map to "Human Resources Staff."
  (Ein Benutzer muss also der Gruppe „Human Resources" auf dem LDAP Authentifizierungsserver angehören, um der Rolle zugeordnet zu werden.)

Sie denken vermutlich, dass Joe beiden Rollen angehört. Nach der Anmeldung am IVE kann er jedoch nicht auf die Datei- und Secure Meeting-Funktionen zugreifen, die in der Rolle „Human Resources Staff" aktiviert sind. Wenn Sie die Richtlinienverfolgung aktivieren, um die Ursache zu ermitteln, könnten beispielsweise die folgenden Protokolleinträge angezeigt werden:

Severity	ID	Message
Info	PTR10103	2004/01/28 17:52:40 - ive-2 - [10.12.254.193] admin03(Admin Users)[.Administrators] - joe:human resources realm - Policy Tracing turned on
Info	PTR22787	2004/01/28 17:53:12 - ive-2 - [10.12.254.193] joe(human resources realm) - Successful authentication with auth server 'human resources server'
Info	PTR10209	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Realm human resources realm running 2 mapping rules for user joe
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable user = "joe"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable sourceIp = 10.12.254.193
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable userAgent = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable loginTime = Wed Jan 28 17:53:12 2004
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable networkIf = "internal"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable realm = "human resources realm"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable auth = "human resources server"
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable hostCheckerPolicy =
Info	PTR10217	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Variable cacheCleanerStatus = 0
Info	PTR10212	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Mapped to roles All Employees by rule 'user = '*''
Info	PTR10218	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - No match on rule 'group.humanresources'
Info	PTR10218	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - No match on rule 'group.humanresources'
Info	PTR10205	2004/01/28 17:53:12 - ive-2 - joe(human resources realm) - Realm human resources realm mapped user joe to roles All Employees

Beim Durchgehen der Verfolgungsdatei sehen Sie, dass das Problem in Eintrag PTR10218 liegt:

```
joe(human resources realm)-No match on rule 'group.humanresources'
```

Dieser Eintrag zeigt, dass das IVE Joe nicht der Rolle „Human Resource Staff" zugeordnet hat, weil er kein Mitglied der Gruppe „Human Resources" auf dem LDAP-Server ist.

So erstellen Sie eine Richtlinienverfolgungsdatei:

1. Wählen Sie in der Web console **Maintenance > Troubleshooting > Policy Tracing** aus.
2. Geben Sie im Feld **User** den Namen des Benutzers ein, den Sie verfolgen möchten. Beachten Sie, dass das IVE keine Platzhalter akzeptiert.
3. Wählen Sie im Feld **Realm** den Bereich des Benutzers aus. Auf dem IVE kann kein Bereich ausgewählt werden, der einem anonymen Authentifizierungsserver zugeordnet ist.
4. Klicken Sie auf **Start Recording**. Bitten Sie den Benutzer nach dem Beginn der Aufzeichnung, sich am IVE anzumelden.
5. Klicken Sie zum Anzeigen der Protokolleinträge auf **View Log**.
6. Klicken Sie auf **Stop Recording**, wenn Sie genügend Informationen beisammen haben.
7. Gehen Sie die Meldungen in der Protokolldatei durch, um den Grund für das abweichende Verhalten zu finden. Wenn Sie Problem nicht erkennen und beheben können, klicken Sie auf **Save Log As**, um eine Kopie der Protokolldatei im Netzwerk zu speichern. Senden Sie die Datei anschließend zur Überprüfung an den NetScreen_Support unter `help@support.netscreen.com`.
8. Klicken Sie auf **Clear Log**, um den Inhalt der Protokolldatei zu löschen, oder auf **Delete Trace**, um den Inhalt der Protokolldatei zu löschen und die Standardeinträge aus den Feldern für Benutzername und Bereich zu entfernen.

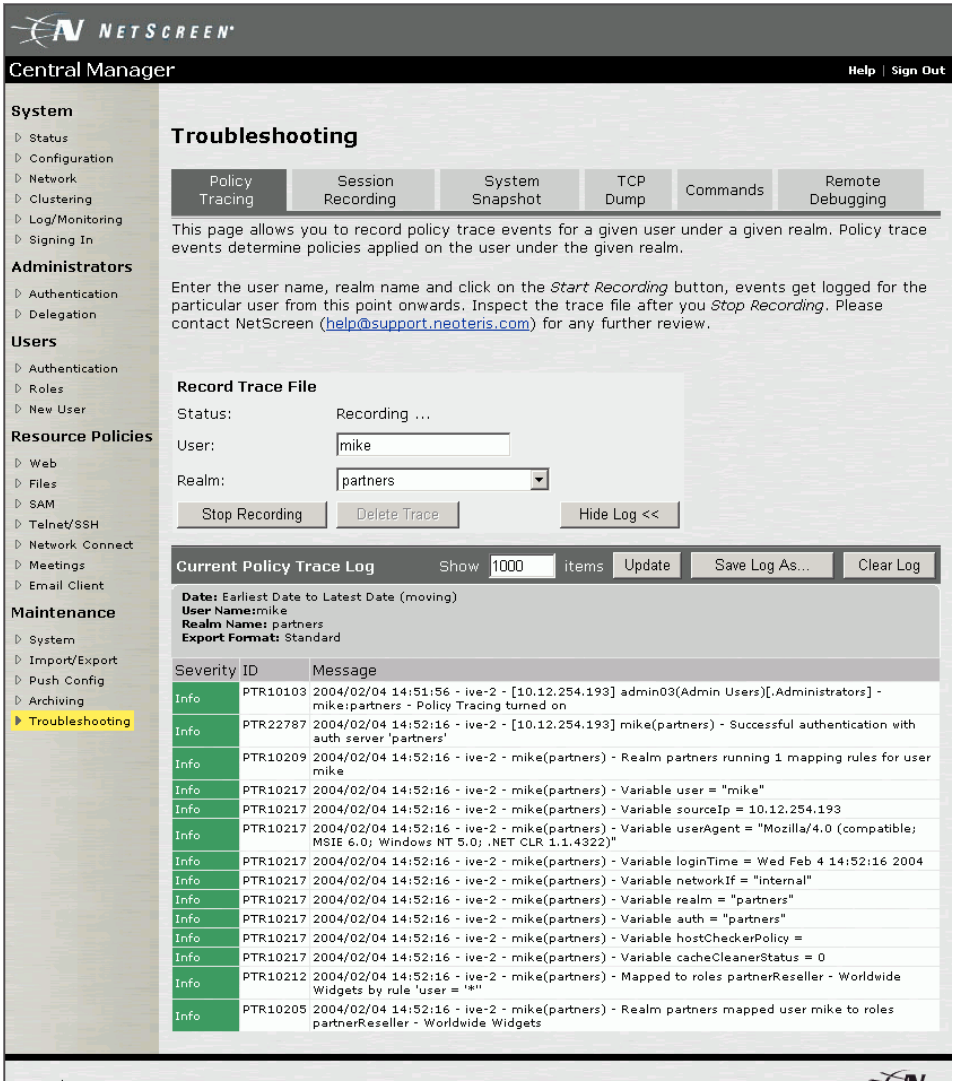

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
SAM
Telnet/SSH
Network Connect
Meetings
Email Client
Maintenance
System
Import/Export
Push Config
Archiving
Troubleshooting
Troubleshooting
Policy Tracing
Session Recording
System Snapshot
TCP Dump
Commands
Remote Debugging
This page allows you to record policy trace events for a given user under a given realm. Policy trace events determine policies applied on the user under the given realm.
Enter the user name, realm name and click on the Start Recording button, events get logged for the particular user from this point onwards. Inspect the trace file after you Stop Recording. Please contact NetScreen (help@support.neoteris.com) for any further review.
Record Trace File
Status: Recording ...
User: mike
Realm: partners
Stop Recording
Delete Trace
Hide Log <<
Current Policy Trace Log
Show 1000 items
Update
Save Log As...
Clear Log
Date: Earliest Date to Latest Date (moving)
User Name:mike
Realm Name: partners
Export Format: Standard
Severity ID Message
Info PTR10103 2004/02/04 14:51:56 - ive-2 - [10.12.254.193] admin03(Admin Users)[.Administrators] - mike:partners - Policy Tracing turned on
Info PTR22787 2004/02/04 14:52:16 - ive-2 - [10.12.254.193] mike(partners) - Successful authentication with auth server 'partners'
Info PTR10209 2004/02/04 14:52:16 - ive-2 - mike(partners) - Realm partners running 1 mapping rules for user mike
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable user = "mike"
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable sourceIp = 10.12.254.193
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable userAgent = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)"
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable loginTime = Wed Feb 4 14:52:16 2004
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable networkIf = "internal"
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable realm = "partners"
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable auth = "partners"
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable hostCheckerPolicy =
Info PTR10217 2004/02/04 14:52:16 - ive-2 - mike(partners) - Variable cacheCleanerStatus = 0
Info PTR10212 2004/02/04 14:52:16 - ive-2 - mike(partners) - Mapped to roles partnerReseller - Worldwide Widgets by rule 'user = '*''
Info PTR10205 2004/02/04 14:52:16 - ive-2 - mike(partners) - Realm partners mapped user mike to roles partnerReseller - Worldwide Widgets

Abbildung 121: Maintenance > Troubleshooting > Policy Tracing

Registerkarte „Session Recording“

☑ Aufzeichnen einer Ablaufverfolgungsdatei zur Fehlerbehebung

Auf dieser Registerkarte können Sie eine Ablaufverfolgungsdatei aufzeichnen, in der die Aktionen eines Benutzers beim Navigieren zu einer Website aufgeführt werden, die über das IVE nicht ordnungsgemäß angezeigt wird. Wenn Sie diese Option verwenden, erzwingt das IVE eine erneute Anmeldung des angegebenen Benutzers und beginnt dann mit der Aufzeichnung sämtlicher Benutzeraktionen. Beachten Sie, dass das IVE die Benutzer über die Aufzeichnung der Benutzeraktionen benachrichtigt.

So zeichnen Sie eine Ablaufverfolgungsdatei auf:

1. Wählen Sie in der Web console **Maintenance > Troubleshooting > Session Recording** aus.
2. Geben Sie den Benutzernamen des Benutzers ein, und klicken Sie auf **Start Recording**.
3. Weisen Sie den Benutzer an, zu der problematischen Website zu navigieren.
4. Klicken Sie auf **Stop Recording**.
5. Klicken Sie auf **dsrecord.log**, um die Datei auf einen Netzwerkcomputer herunterzuladen. Entfernen Sie alle vertraulichen Daten mithilfe eines Text-Editors.
6. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: `help@support.netscreen.com`.

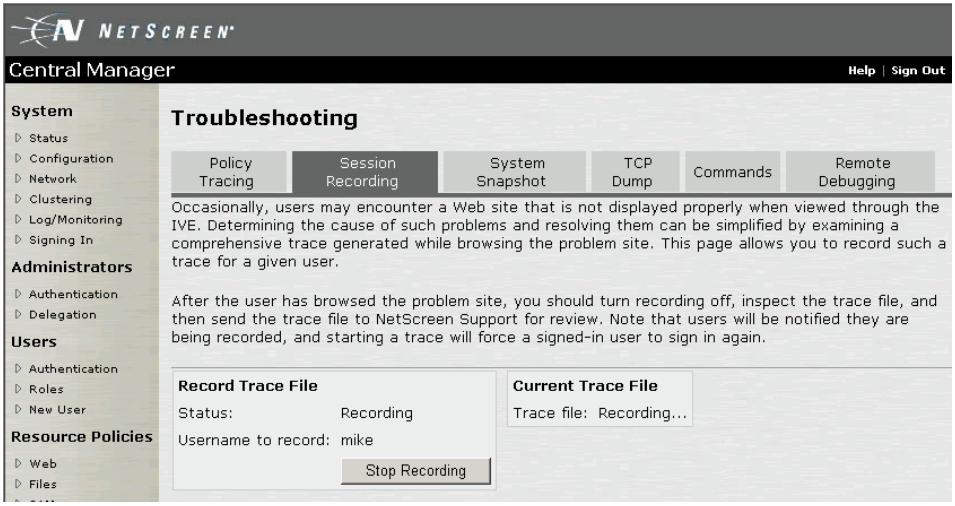

NETSCREEN
Central Manager
Help | Sign Out
System
Status
Configuration
Network
Clustering
Log/Monitoring
Signing In
Administrators
Authentication
Delegation
Users
Authentication
Roles
New User
Resource Policies
Web
Files
Troubleshooting
Policy Tracing
Session Recording
System Snapshot
TCP Dump
Commands
Remote Debugging
Occasionally, users may encounter a Web site that is not displayed properly when viewed through the IVE. Determining the cause of such problems and resolving them can be simplified by examining a comprehensive trace generated while browsing the problem site. This page allows you to record such a trace for a given user.
After the user has browsed the problem site, you should turn recording off, inspect the trace file, and then send the trace file to NetScreen Support for review. Note that users will be notified they are being recorded, and starting a trace will force a signed-in user to sign in again.
Record Trace File
Status: Recording
Username to record: mike
Stop Recording
Current Trace File
Trace file: Recording...

Abbildung 122: Maintenance > Troubleshooting > Session Recording

Registerkarte „System Snapshot“

☑ Erstellen eines Snapshots des IVE-Systemstatus

Auf dieser Registerkarte können Sie einen Snapshot des IVE-Systemstatus erstellen. Wenn Sie diese Option verwenden, führt das IVE verschiedene Dienstprogramme aus, um Details zum IVE-Systemstatus zu erfassen, beispielsweise zum belegten Speicherplatz, zur Auslagerungsleistung, zur Anzahl der ausgeführten Prozesse, zur Systembetriebszeit, zur Anzahl der geöffneten Dateibeschreibungen, zu den verwendeten Ports und zu den Access Series FIPS-Protokollmeldungen. Das IVE speichert bis zu zehn Snapshots, die in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei abgelegt werden. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den NetScreen Support senden.

So erstellen Sie einen Snapshot des IVE-Systemstatus:

1. Wählen Sie in der Web console **Maintenance > Troubleshooting > System Snapshot** aus.
2. Klicken Sie auf **Take Snapshot**.

3. Wenn das IVE das Erstellen des Snapshots beendet hat, klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
4. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: `help@support.netscreen.com`.

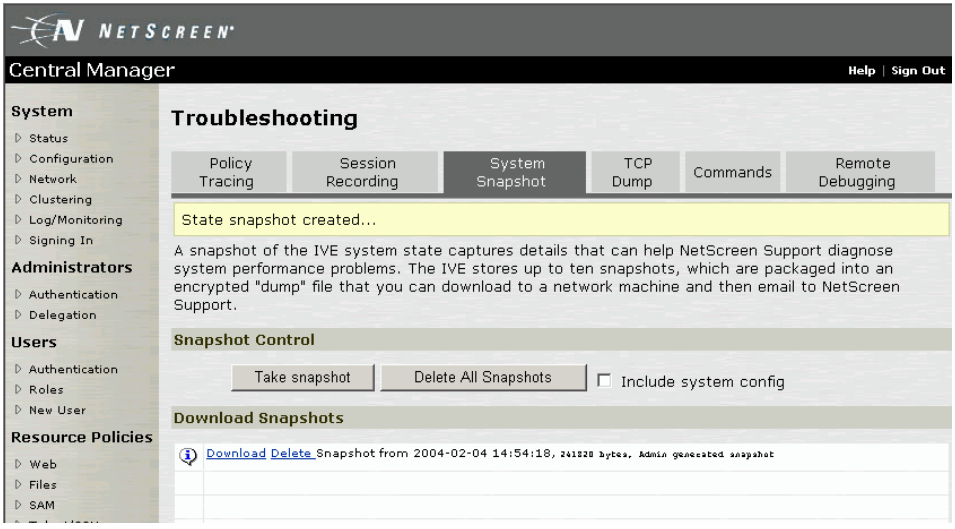


Abbildung 123: Maintenance > Troubleshooting > System Snapshot

Registerkarte „TCP Dump“

☑ Sniffing von Netzwerkpaketheadern

Auf dieser Registerkarte können Sie Sniffing von Netzwerkpaketheadern durchführen und die Ergebnisse in einer verschlüsselten „Dumpdatei“ bzw. Sicherungsdatei speichern. Diese können Sie auf einen Netzwerkcomputer herunterladen und dann per E-Mail an den NetScreen Support senden.

So führen Sie Sniffing von Netzwerkpaketheadern durch:

1. Wählen Sie in der Web console **Maintenance > Troubleshooting > TCP Dump** aus.
2. Wählen Sie den IVE-Port aus, an dem Sniffing von Netzwerkpaketheadern durchgeführt werden soll.
3. Deaktivieren Sie den **Promiscuous**-Modus, sodass Sniffing nur für Pakete durchgeführt wird, die für das IVE bestimmt sind.

4. Klicken Sie auf **Start Sniffing**.
5. Klicken Sie auf **Stop Sniffing**, um das Sniffing zu beenden und eine verschlüsselte Datei zu erstellen.
6. Klicken Sie auf **Download**, um die Datei auf einen Netzwerkcomputer herunterzuladen.
7. Senden Sie die Datei zur Überprüfung per E-Mail an die folgende Adresse: `help@support.netscreen.com`.

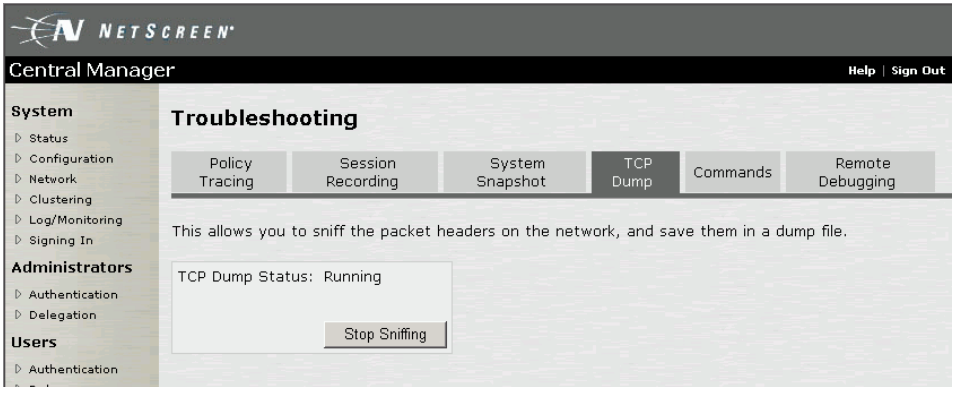


Abbildung 124: Maintenance > Troubleshooting > TCP Dump (Erstellung einer Dumpdatei)

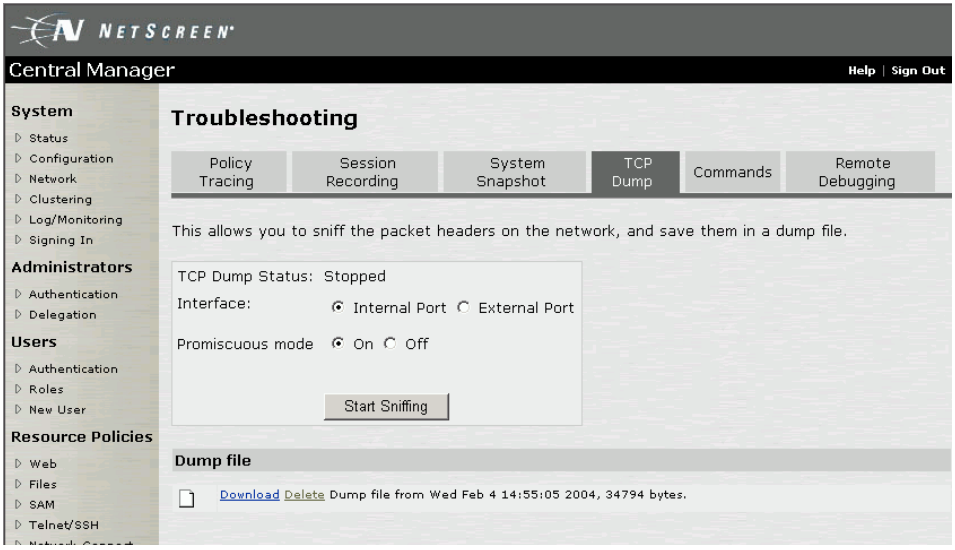


Abbildung 125: Maintenance > Troubleshooting > TCP Dump (nach Erstellung einer Dumpdatei)

Registerkarte „Commands“

☑ Ausführen eines ARP-, ping-, traceroute- oder nslookup-Befehls

Auf dieser Registerkarte können Sie UNIX-Befehle ausführen, um die IVE-Netzwerkverbindung zu testen.

So führen Sie einen UNIX-Befehl aus, um die IVE-Netzwerkverbindung zu testen:

1. Wählen Sie in der Web console **Maintenance > Troubleshooting > Commands** aus.
2. Wählen Sie in der Liste **Command** den Befehl aus, der ausgeführt werden soll.
3. Geben Sie im Feld **Target Server** die IP-Adresse des Zielservers ein.
4. Klicken Sie zur Ausführung des Befehls auf **OK**.

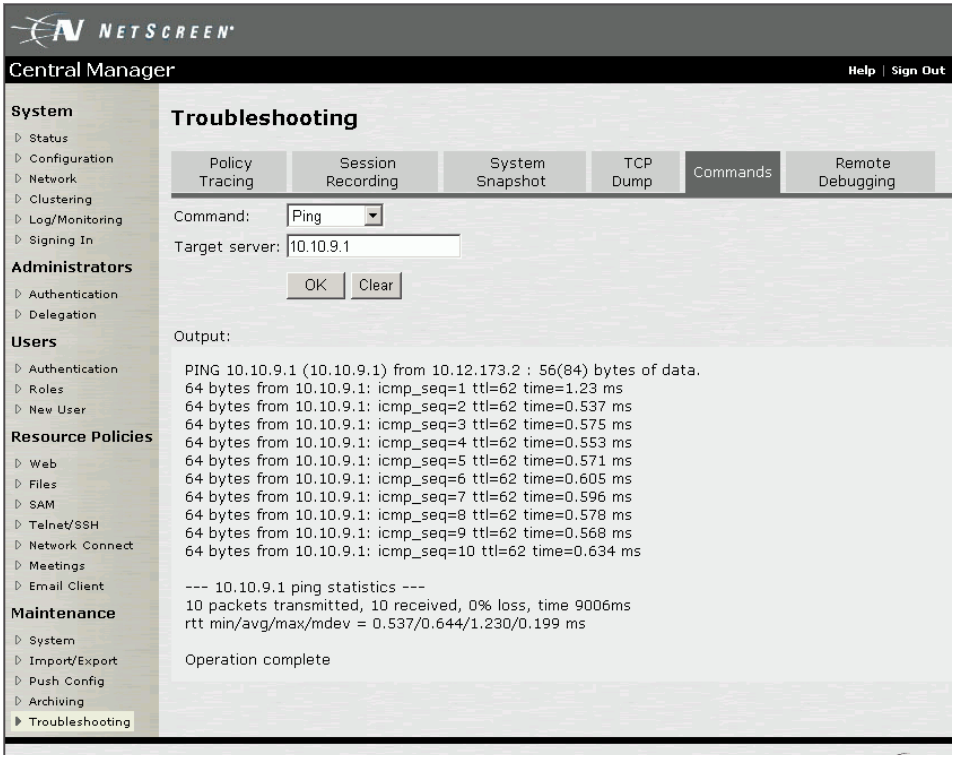


Abbildung 126: **Maintenance > Troubleshooting > Commands**

Registerkarte „Remote Debugging“

☑ Aktivieren von Remotefehlerbehebung für den NetScreen Support

Auf dieser Registerkarte können Sie es dem NetScreen Support-Team ermöglichen, auf Ihrem Produktions-IVE Tools für die Fehlerbehebung auszuführen. Zur Aktivierung dieser Option müssen Sie mit dem NetScreen Support zusammenarbeiten. Sie erhalten dann einen Code für die Fehlerbehebung und einen Host, mit dem das IVE eine Verbindung herstellt.

So aktivieren Sie Remotefehlerbehebung:

1. Wenden Sie sich an den NetScreen Support, um die Bedingungen für eine Remotesitzung zur Fehlerbehebung einzurichten.
2. Wählen Sie in der Web console **Maintenance > Troubleshooting > Remote Debugging** aus.

3. Geben Sie den Fehlerbehebungscode ein, den Sie vom NetScreen Support erhalten haben.
4. Geben Sie den Hostnamen ein, den Sie vom NetScreen Support erhalten haben.
5. Klicken Sie auf **Enable Debugging**, sodass das NetScreen Support-Team auf das IVE zugreifen kann.
6. Teilen Sie dem NetScreen Support mit, dass auf Ihr IVE zugegriffen werden kann.
7. Klicken Sie auf **Disable Debugging**, wenn der NetScreen Support Ihnen mitteilt, dass die Remotesitzung zur Fehlerbehebung beendet ist.

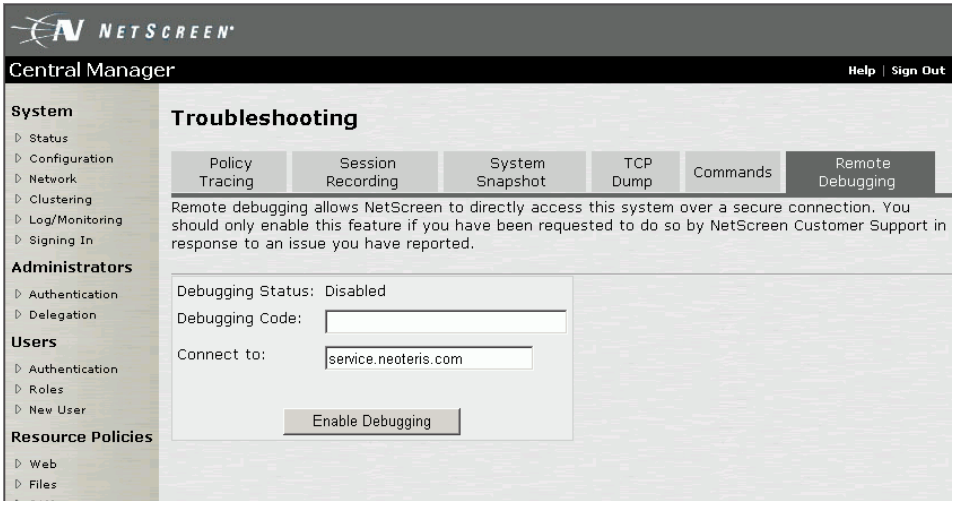


Abbildung 127: Maintenance > Troubleshooting > Remote Debugging

Chapter 4
Zusatzinformationen

In diesem Abschnitt finden Sie weiterführende Informationen zur Konfiguration von Access Series-Produkten.

Inhalt

Authentifizierung und Autorisierung – Flussdiagramm....423
Konfigurieren der Zugriffsverwaltungsoptionen....427
Schreiben benutzerdefinierter Ausdrücke....437
Verwenden der seriellen Konsole des IVE....453

Appendix A.

Authentifizierung und Autorisierung – Flussdiagramm

In diesem Flussdiagramm werden die Transaktionen zwischen Benutzer und IVE sowie zwischen IVE und Authentifizierungsbereich dargestellt. Das Flussdiagramm beginnt an dem Punkt, an dem ein Benutzer in der IVE-Anmeldungsseite einen URL eingibt und endet damit, dass der Benutzer die Benutzersitzung eigenständig beendet.

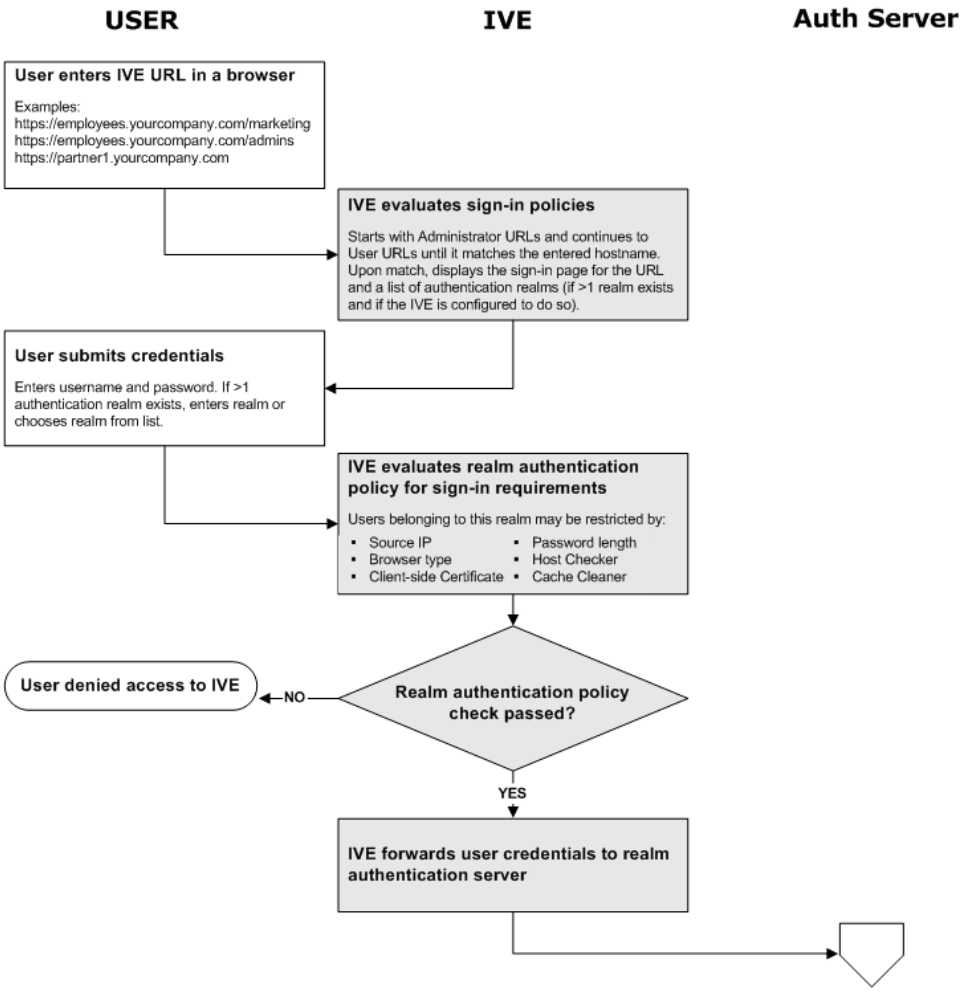

USER
IVE
Auth Server
User enters IVE URL in a browser
Examples:
https://employees.yourcompany.com/marketing
https://employees.yourcompany.com/admins
https://partner1.yourcompany.com
IVE evaluates sign-in policies
Starts with Administrator URLs and continues to User URLs until it matches the entered hostname. Upon match, displays the sign-in page for the URL and a list of authentication realms (if >1 realm exists and if the IVE is configured to do so).
User submits credentials
Enters username and password. If >1 authentication realm exists, enters realm or chooses realm from list.
IVE evaluates realm authentication policy for sign-in requirements
Users belonging to this realm may be restricted by:
Source IP
Browser type
Client-side Certificate
Password length
Host Checker
Cache Cleaner
Realm authentication policy check passed?
NO
User denied access to IVE
YES
IVE forwards user credentials to realm authentication server

Abbildung 128: **Schritt 1 von 3: IVE authentifiziert Benutzer**

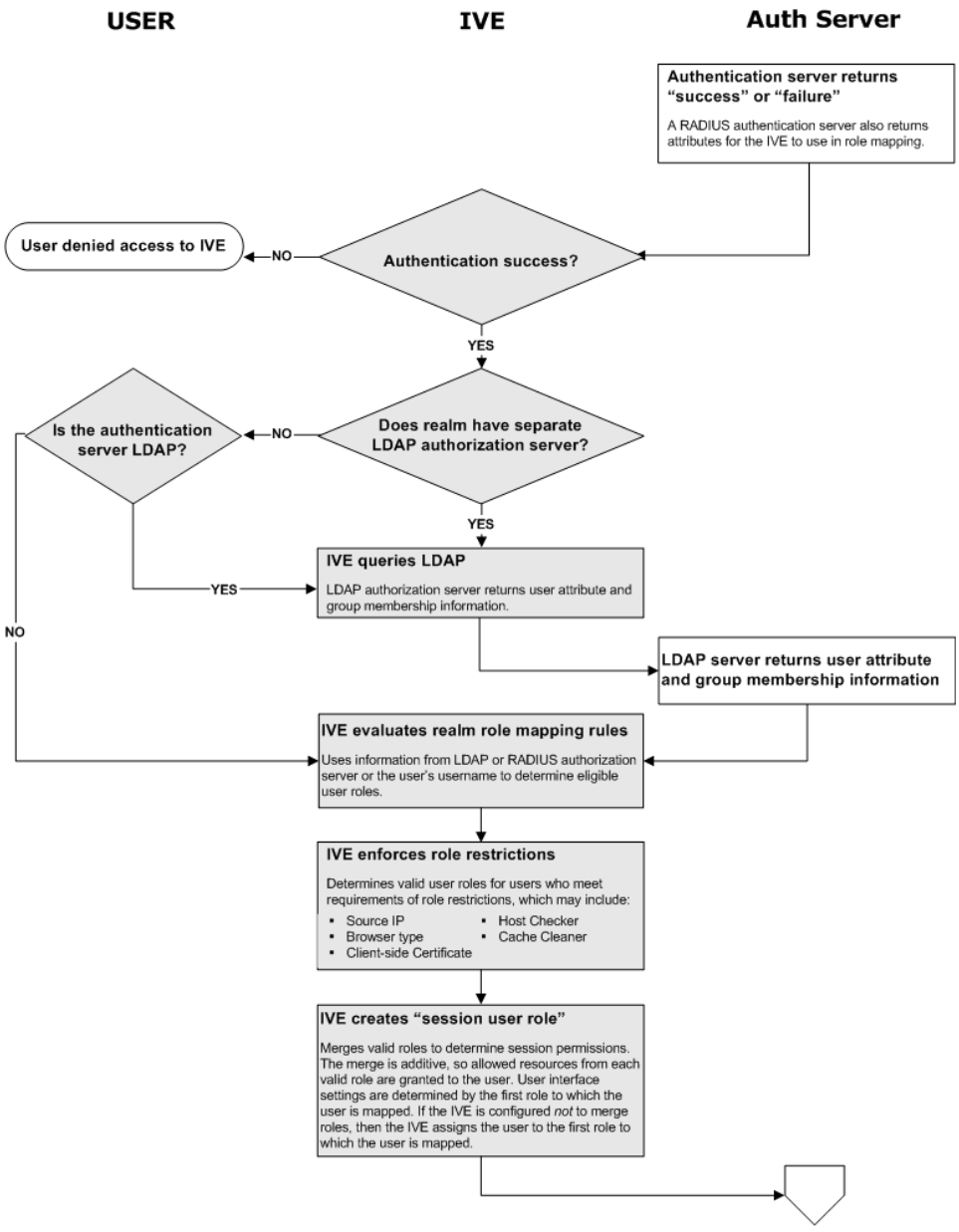

USER
IVE
Auth Server
Authentication server returns "success" or "failure"
A RADIUS authentication server also returns attributes for the IVE to use in role mapping.
User denied access to IVE
NO
Authentication success?
YES
Is the authentication server LDAP?
NO
Does realm have separate LDAP authorization server?
YES
YES
IVE queries LDAP
LDAP authorization server returns user attribute and group membership information.
NO
LDAP server returns user attribute and group membership information
IVE evaluates realm role mapping rules
Uses information from LDAP or RADIUS authorization server or the user's username to determine eligible user roles.
IVE enforces role restrictions
Determines valid user roles for users who meet requirements of role restrictions, which may include:
Source IP
Browser type
Client-side Certificate
Host Checker
Cache Cleaner
IVE creates "session user role"
Merges valid roles to determine session permissions. The merge is additive, so allowed resources from each valid role are granted to the user. User interface settings are determined by the first role to which the user is mapped. If the IVE is configured *not* to merge roles, then the IVE assigns the user to the first role to which the user is mapped.

Abbildung 129: Schritt 2 von 3: IVE ordnet den Benutzer zu einer oder mehreren Rollen zu

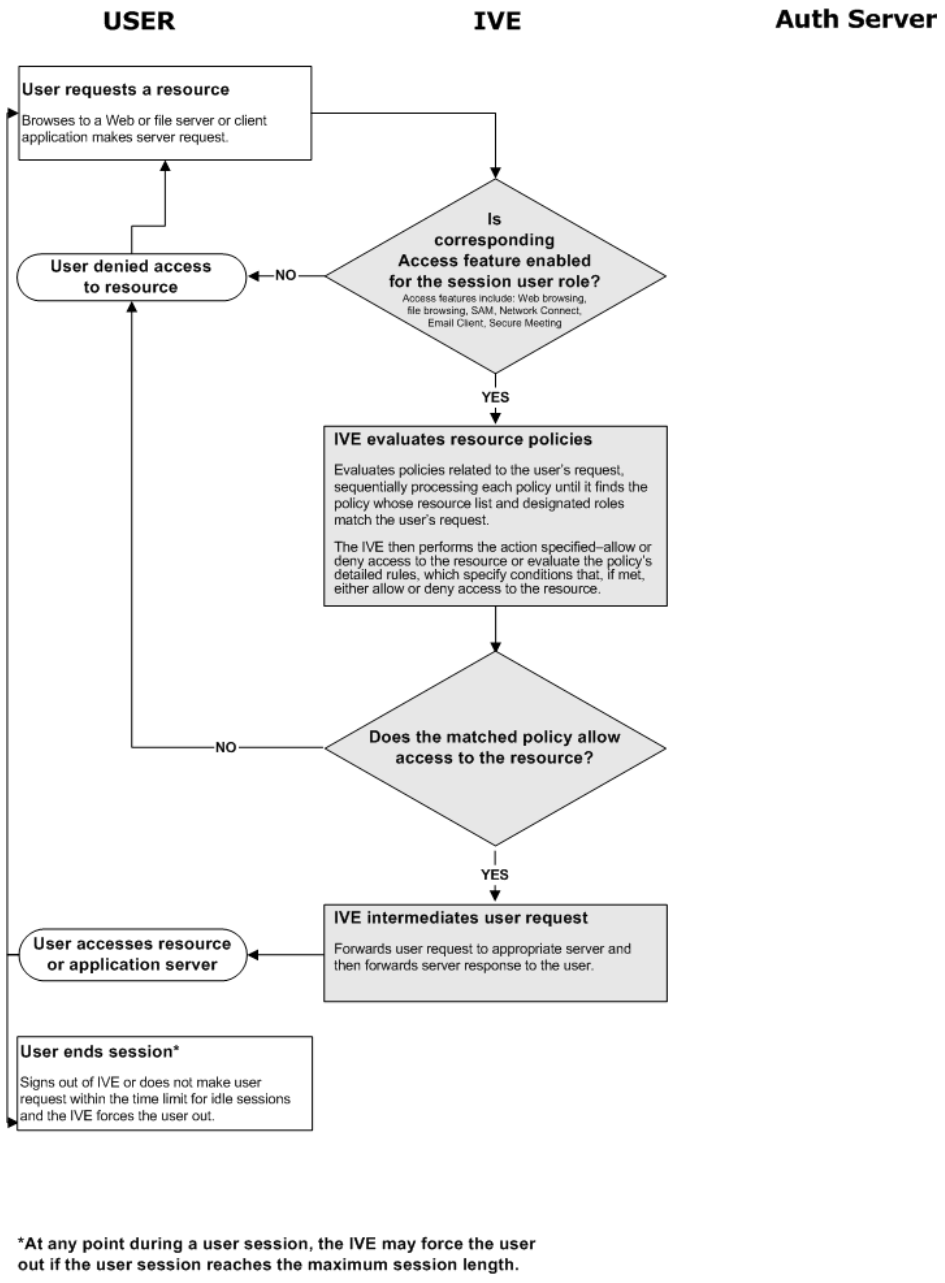

USER
IVE
Auth Server
User requests a resource
Browses to a Web or file server or client application makes server request.
Is corresponding Access feature enabled for the session user role?
Access features include: Web browsing, file browsing, SAM, Network Connect, Email Client, Secure Meeting
NO
User denied access to resource
YES
IVE evaluates resource policies
Evaluates policies related to the user's request, sequentially processing each policy until it finds the policy whose resource list and designated roles match the user's request.
The IVE then performs the action specified–allow or deny access to the resource or evaluate the policy's detailed rules, which specify conditions that, if met, either allow or deny access to the resource.
Does the matched policy allow access to the resource?
NO
YES
IVE intermediates user request
Forwards user request to appropriate server and then forwards server response to the user.
User accesses resource or application server
User ends session*
Signs out of IVE or does not make user request within the time limit for idle sessions and the IVE forces the user out.
*At any point during a user session, the IVE may force the user out if the user session reaches the maximum session length.

Abbildung 130: Schritt 3 von 3: IVE wertet die Ressourcenrichtlinien entsprechend der Benutzeranforderung aus

Appendix B.

Konfigurieren der Zugriffsverwaltungsoptionen

Das IVE ermöglicht Ihnen die Sicherung Ihrer Unternehmensressourcen auf drei Ebenen:

- **Bereich**

  Auf der Bereichsebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung in der Authentifizierungsrichtlinie.

- **Rolle**

  Auf der Rollenebene konfigurieren Sie die Anforderungen für die Zugriffsverwaltung entweder in den Rollenzuordnungsregeln der Authentifizierungsrichtlinie oder über die Einschränkungsoptionen für die Rolle.

- **Ressourcenrichtlinie**

  Auf der Ebene der Ressourcenrichtlinie konfigurieren Sie die Anforderungen für die Zugriffsverwaltung, indem Sie Bedingungen für Rollen schreiben.

Konfigurationsanweisungen für Optionen der Zugriffsverwaltung finden Sie unter:

Angeben von Quell-IP-Einschränkungen 428
Angeben von Browsereinschränkungen 429
Angeben clientseitiger Zertifikateinschränkungen 432
Angeben einer Kennwortlängeneinschränkung 433
Angeben von Hostprüfungseinschränkungen 434
Angeben von Quell-IP-Einschränkungen 428
Angeben von Quell-IP-Einschränkungen 428

Übersichtsinformationen finden Sie unter „Zugriffsverwaltung – Übersicht“ auf Seite 23.

Quell-IP-Einschränkungen

Mit einer Quell-IP-Einschränkung kann gesteuert werden, von welcher IP-Adresse aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können.

☑ Angeben von Quell-IP-Einschränkungen

So geben Sie Quell-IP-Einschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Source IP

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Source IP
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Source IP

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Users can sign in from any IP address** – Hiermit können sich Benutzer von einer beliebigen IP-Adresse aus beim IVE anmelden, um die Anforderungen für die Zugriffsverwaltung zu erfüllen.
- **Users can only sign in from the following IP addresses** – Schränkt die Anzahl der IP-Adressen ein, von denen aus sich Benutzer anmelden können, um die Anforderungen für die Zugriffsverwaltung

zu erfüllen. Wenn Sie diese Option auswählen, müssen Sie mindestens eine IP-Adresse angeben, da sonst keine Quell-IP-Einschränkung angewendet werden kann.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Browsereinschränkungen

Mit einer Browsereinschränkung kann gesteuert werden, von welchen Webbrowsern aus Benutzer auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden können. Wenn ein Benutzer versucht, sich im IVE über einen nicht unterstützten Browser anzumelden, schlägt der Anmeldeversuch fehl, und es wird in einer Meldung angezeigt, dass ein nicht unterstützter Browser verwendet wird. Mit dieser Funktion können Sie auch sicherstellen, dass sich Benutzer im IVE über Browser anmelden, die mit Firmenanwendungen kompatibel oder von Firmensicherheitsrichtlinien zugelassen sind.

Hinweis: Das Feature zur Browsereinschränkung dient nicht als strikte Zugriffssteuerung, da die Benutzer-Agent-Zeichenfolgen des Browsers von einem technischen Benutzer geändert werden können. Es dient als beratende Zugriffssteuerung für normale Nutzungsszenarien.

☑ Angeben von Browsereinschränkungen

So geben Sie Browsereinschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Browser

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Browser
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Browser

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users matching any user-agent string sent by the browser** – Ermöglicht Benutzern den Zugriff auf das IVE oder auf Ressourcen mit einem beliebigen unterstützten Webbrowser.
- **Only allow users matching based on the user-agent string sent by the browser** – Ermöglicht Ihnen die Definition von Regeln für die Browserzugriffssteuerung. So erstellen Sie eine Regel:

  1. Geben Sie für **User-agent string pattern** eine Zeichenfolge in folgendem Format ein:

     `*<browser_zeichenfolge>*`

     wobei Start (`*`) ein optionales Zeichen ist, das für ein beliebiges Zeichen steht, und `<browser_zeichenfolge>` ein Muster darstellt (Groß- und Kleinschreibung wird berücksichtigt), das mit einer Teilzeichenfolge im „User-Agent"-Header übereinstimmen muss, der vom Browser gesendet wurde.

  2. Wählen Sie eine der folgenden Optionen aus:
     Allow, um Benutzern die Verwendung eines Browsers mit einem „User-Agent"-Header zu ermöglichen, der die Teilzeichenfolge `<browser_zeichenfolge>` enthält, oder
     Deny, um Benutzern die Verwendung eines Browsers mit einem „User-Agent"-Header zu verweigern, der die Teilzeichenfolge `<browser_zeichenfolge>` enthält.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

- Regeln werden der Reihenfolge nach angewendet, d.h., die erste übereinstimmende Regel wird angewendet.
- Bei Literalzeichen in Regeln wird die Groß- und Kleinschreibung beachtet, Leerzeichen sind dabei zulässig.

Beispiele

- Die Zeichenfolge `*Netscape*` findet für alle für Benutzer-Agent-Zeichenfolgen eine Übereinstimmung, die die Teilzeichenfolge `Netscape` enthält.
- Der folgende Regelsatz ermöglicht Ressourcenzugriff nur dann, wenn Benutzer über Internet Explorer 5.5x oder Internet Explorer 6.x angemeldet sind. In diesem Beispiel werden einige wichtige andere Browser als Internet Explorer berücksichtigt, die die Teilzeichenfolge „MSIE" im „User-Agent"-Header senden:

  `*Opera*` **Deny**

  `*AOL*` **Deny**

  `*MSIE 5.5*` **Allow**

  `*MSIE 6.*` **Allow**

  `*` **Deny**

Zertifikateinschränkungen

Legen Sie anhand einer Zertifikateinschränkung fest, dass Clientcomputer über ein gültiges clientseitiges Zertifikat verfügen müssen, um auf eine IVE-Anmeldeseite oder eine Ressource zugreifen oder einer Rolle zugeordnet werden zu können. Wenn Sie dieses Feature verwenden, stellen Sie sicher, dass Sie ein Stammzertifikat importieren, um das clientseitige Zertifikat zu überprüfen. Um die Sicherheit dieses Features zu optimieren, sollten die Clienteinstellungen eines Benutzers so festgelegt werden, dass der Benutzer bei jeder Anmeldung ein Kennwort eingeben muss. In der Standardeinstellung wird bei einigen Browserversionen das Zertifikatkennwort gespeichert, d.h. der Benutzer wird nach Installation des Zertifikats nicht zur Eingabe dieser zusätzlichen Anmeldeinformationen aufgefordert.

☑ Angeben clientseitiger Zertifikateinschränkungen

So geben Sie Zertifikateinschränkungen auf den unterschiedlichen Ebenen an:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Certificate

- **Rollenebene**

  Navigieren Sie zu:

  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Certificate
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Certificate

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users (no client-side certificate required)** – Clients von Benutzern müssen nicht über ein clientseitiges Zertifikat verfügen.
- **Only allow users with a client-side certificate signed by Certification Authority to sign in** – Legt fest, dass der Client eines Benutzers über ein clientseitiges Zertifikat verfügen muss, um die Anforderungen für die Zugriffsverwaltung zu erfüllen. Um den Zugriff noch weiter einzuschränken, können Sie eindeutige Attribut-Wert-Paare für das Zertifikat festlegen.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

- Alle X.509-DN-Attribute (Distinguished Name) werden unterstützt (z.B. C, CN, L, O, OU).
- Bei den Attribut- und Wertefeldern wird die Groß- und Kleinschreibung nicht beachtet.
- Definieren Sie für jedes Attribut nur einen Wert. Wenn Sie mehrere Werte angeben, kann das clientseitige Zertifikat möglicherweise nicht ordnungsgemäß anhand des Stammzertifikats authentifiziert werden.

Kennworteinschränkung

Verwenden Sie eine Kennworteinschränkung, um eine minimale erforderliche Kennwortlänge für den Bereich festzulegen.

☑ Angeben einer Kennwortlängeneinschränkung

So geben Sie eine Kennworteinschränkung auf der Bereichsebene ein:

Navigieren Sie zu:

- Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password
- Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Password

Gehen Sie anschließend folgendermaßen vor:

Wählen Sie eine der folgenden Optionen aus:

- **Allow all users (passwords of any length)** – Für Benutzer, die sich beim IVE anmelden, wird keine Kennwortlängeneinschränkung angewendet.
- **Only allow users that have passwords of a minimum length** – Bei dieser Option muss das einzugebende Kennwort eine festgelegte Anzahl von Zeichen lang sein.

Klicken Sie zum Speichern der Einstellungen auf **Save Changes**.

Hinweis

Für das IVE müssen die auf der Anmeldeseite eingegebenen Benutzerkennwörter standardmäßig mindestens vier Zeichen lang sein. Für den zur Überprüfung der Anmeldeinformationen eines Benutzers verwendeten Authentifizierungsserver ist unter Umständen eine andere Mindestlänge erforderlich. Für die lokale Authentifizierungsdatenbank von IVE müssen die Benutzerkennwörter beispielsweise mindestens sechs Zeichen lang sein.

Hostprüfungseinstellungen

Legen Sie anhand einer Hostprüfungseinschränkung fest, dass Clientcomputer die angegebenen Hostprüfungsrichtlinien erfüllen müssen, um auf eine IVE-Anmeldeseite oder eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden zu können.

☑ Angeben von Hostprüfungseinschränkungen

So geben Sie Hostprüfungseinschränkungen an:

Systemweite Richtlinien für die Hostprüfung werden folgendermaßen angegeben:
System > Configuration > Security > Hostprüfung

Gehen Sie dann in den einzelnen Bereichen folgendermaßen vor:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Hostprüfung

- **Rollenebene**
  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte*|*erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Hostprüfung

- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte*|*Erstellte Regel* > *Bedingungsfeld*

Nächster Schritt:

Wenn Sie eine Hostprüfung-Anforderung der ***Bereichsebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Allow all users** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Hostprüfung nicht installiert ist.

- **Allow all users & install Host Checker** – Legt fest, dass das IVE die Hostprüfung auf den Clientcomputer herunterladen muss.
- **Allow only users whose workstations meet the requirements specified by the following** [Richtlinien] – Der Benutzer erfüllt die Zugriffsvoraussetzungen nur, wenn die Hostprüfung die angegebene Richtlinie für die Hostprüfung ausführt.

Wenn Sie eine Hostprüfung-Anforderung auf ***Rollenebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Allow all users** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Hostprüfung nicht installiert ist.
- **Allow only users whose workstations meet the requirements specified by the following** [Richtlinien] – Der Benutzer erfüllt die Zugriffsvoraussetzungen nur, wenn die Hostprüfung die angegebene Richtlinie für die Hostprüfung ausführt.

Sie können auch einen benutzerdefinierten Ausdruck für die Rollenzuordnungsregel schreiben, um den Status von Hostprüfung anhand der Variable `hostCheckerPolicy` auszuwerten. Zum Erstellen von Hostprüfung-Einschränkungen auf der ***Ressourcenrichtlinienebene*** müssen Sie einen benutzerdefinierten Ausdruck in einer detaillierten Regel erstellen.

Cachebereinigungseinschränkungen

Legen Sie anhand einer Cachebereinigungseinschränkung fest, dass Clientcomputer die angegebenen Cachebereinigungsrichtlinien erfüllen müssen, um auf eine IVE-Anmeldeseite bzw. eine Ressourcenrichtlinie zugreifen oder einer Rolle zugeordnet werden zu können.

☑ Angeben von Cachebereinigungseinschränkungen

So geben Sie Cachebereinigungseinschränkungen an:

Systemweite Richtlinien für die Hostprüfung werden folgendermaßen angegeben:
System > Configuration > Security > Hostprüfung

Gehen Sie dann in den einzelnen Bereichen folgendermaßen vor:

- **Bereichsebene**

  Navigieren Sie zu:

  - Administrators > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cache Cleaner
  - Users > Authentication > *Ausgewählter Bereich* > Authentication Policy > Cache Cleaner

- **Rollenebene**
  - Administrators > Delegation > *Ausgewählte Rolle* > General > Restrictions > Cache Cleaner
  - Users > Authentication > *Ausgewählter Bereich* > Role Mapping > *Ausgewählte|erstellte Regel* > *Benutzerdefinierter Ausdruck*
  - Users > Roles > *Ausgewählte Rolle* > General > Restrictions > Cache Cleaner
- **Ressourcenrichtlinienebene**

  Navigieren Sie zu:

  Resource Policies > *Ausgewählte Ressource* > *Ausgewählte Richtlinie* > Detailed Rules > *Ausgewählte|Erstellte Regel* > *Bedingungsfeld*

Nächster Schritt:

Wenn Sie eine Cachebereinigungsanforderung auf ***Bereichsebene*** konfigurieren, wählen Sie eine der folgenden Optionen aus:

- **Just load Cache Cleaner** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Cachebereinigung nicht ausgeführt wird, diese ist jedoch für eine spätere Verwendung verfügbar.
- **Load and enforce Cache** – Der Benutzer erfüllt die Zugriffsanforderungen nur, wenn das IVE die Cachebereinigung herunterlädt und ausführt.
- **Diasble Cache Cleaner** – Der Benutzer erfüllt die Zugriffsvoraussetzungen auch dann, wenn die Cachebereinigung nicht installiert ist.

Aktivieren Sie zum Konfigurieren einer Cachebereinigungsanforderung auf ***Rollenebene*** die folgende Option:

- **Enable Cache Cleaner** – Der Benutzer erfüllt die Zugriffsanforderungen nur, wenn die Cachebereinigung ausgeführt wird.

Sie können auch einen benutzerdefinierten Ausdruck für die Rollenzuordnungsregel schreiben, um den Status der Cachebereinigung anhand der Variable `cacheCleaner` auszuwerten. Zum Erstellen einer Cachebereinigungseinschränkung auf der ***Ressourcenrichtlinienebene*** müssen Sie einen benutzerdefinierten Ausdruck in einer detaillierten Regel erstellen.

Appendix C.

Schreiben benutzerdefinierter Ausdrücke

Mit dem IVE können Sie benutzerdefinierte Ausdrücke schreiben, die in Rollenzuordnungsregeln, Ressourcenrichtlinien und Protokollfilterabfragen ausgewertet werden. Ein ***benutzerdefinierter Ausdruck*** ist eine Kombination von Variablen, die das IVE als boolesches Objekt als „true" (wahr), „false" (falsch)oder error (Fehler) auswertet. Mithilfe von benutzerdefinierten Ausdrücken können Sie komplexe Bedingungen für Richtlinienauswertung und Protokollabfragen erstellen, die die Ressourcenzugriffskontrolle verbessern und erleichtern. Sie können benutzerdefinierte Ausdrücke in den folgenden Formaten schreiben:

Syntax für benutzerdefinierte Ausdrücke

```
variable comparisonOperator variable
variable comparisonOperator simpleValue
variable comparisonOperator (simpleValue)
variable comparisonOperator (ORValues)
variable comparisonOperator (ANDValues)
variable comparisonOperator (time TO time)
variable comparisonOperator (day TO day)
isEmpty (variable)
isUnknown (variable)
(customExpr)
NOT customExpr
! customExpr
customExpr OR customExpr
customExpr || customExpr
customExpr AND customExpr
customExpr && customExpr
```

Dabei gilt Folgendes:

`variable` ist eine Systemvariable. Ein Variablenname ist eine durch Punkte getrennte Zeichenfolge.
Jede Komponente darf Zeichen aus dem Bereich [a-z A-Z 0-9_] enthalten,
darf jedoch nicht mit einer Ziffer [0-9] starten. Bei Variablennamen wird die Groß- und Kleinschreibung nicht berücksichtigt. Informationen zu Systemvariablen, die in Rollenzuordnungsregeln und -ressourcen verwendet werden können,
finden Sie unter „Systemvariablen und Beispiele“ auf Seite 442[a].

`comparisonOperator` kann folgende Werte annehmen:

- `=` gleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden
- `!=` ungleich – Kann für Zeichenfolgen, Zahlen und DNs verwendet werden
- `<` kleiner als – Kann mit Zahlen verwendet werden
- `<=` kleiner oder gleich – Kann mit Zahlen verwendet werden
- `>` größer als – Kann für Zahlen verwendet werden
- `>=` größer oder gleich – Kann für Zahlen verwendet werden

`simpleValue` kann folgende Werte annehmen:

- Zeichenfolge – Zeichenfolge in Anführungszeichen, die Platzhalter enthalten kann
- IP-Adresse – a.b.c.d
- Subnetz – a.b.c.d/Subnetz Anzahl Bits
- Zahl – positive oder negative Ganzzahl
- Tag[b] – SUN MON TUE WED THU FRI SAT

Hinweise zu Zeichenfolgen:

- Eine Zeichenfolge kann alle Zeichen außer <nl> und <cr> enthalten.
- Bei Zeichenfolgenvergleichen wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Zeichenfolgen können in einfache oder doppelte Anführungszeichen gesetzt werden. Eine Zeichenfolge in Anführungsstrichen kann Platzhalter enthalten, d.h. Sternchen (*), Fragezeichen (?) und eckige Klammern ([ ]). Weitere Informationen finden Sie unter „Platzhalterabgleich“ auf Seite 441.
- Vergleiche vom Typ *variable comparisonOperator variable* werden ohne Platzhalterabgleich ausgewertet.
- Verwenden Sie einen umgekehrten Schrägstrich als Escape-Zeichen für die folgenden Zeichen:
  einfaches Anführungszeichen (') – \'
  doppeltes Anführungszeichen (") – \"
  umgekehrter Schrägstrich (\) – \\
  Hexadezimalzahl – \hh [0-9a-fA-F]

`time`[c] ist die Uhrzeit in einem der folgenden Formate:

SS:MM – 24-Stunden-Format
SS:MMam – 12-Stunden-Format
SS:MMpm – 12-Stunden-Format
S:MM – 24-Stunden-Format
S:MMam – 12-Stunden-Format
S:MMpm – 12-Stunden-Format

`ORValue` ist eine Zeichenfolge, die einen oder mehrere OR-Vergleiche enthält:

Variable comparisonOperator (Zahl OR Zahl...)
Variable comparisonOperator (Zeichenfolge OR Zeichenfolge...)

`ANDValue`	ist eine Zeichenfolge, die einen oder mehrere AND-Vergleiche enthält: *`Variable comparisonOperator`* `(Zahl AND Zahl...)` *`Variable comparisonOperator`* `(Zeichenfolge AND Zeichenfolge...)`
`isEmpty`	ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isEmpty() ist „true“, wenn die Variable unbekannt ist, eine Länge von Null hat oder Zeichenfolgen der Länge Null bzw. leere Listen enthält. Beispiel: isEmpty(userAttr.terminationDate)
`isUnknown`	ist eine Funktion, die eine einzelne Variable als Argument nimmt und einen booleschen Wert zurückgibt. isUnknown() ist „true“, wenn die Variable nicht definiert ist. Benutzerattribute (userAttr.*-Variablen) sind unbekannt, wenn das Attribut nicht in LDAP definiert ist oder wenn der Attribut-Lookup fehlschlägt (wenn z. B. der LDAP-Server außer Betrieb ist). Beispiel: isUnknown(userAttr.bonusProgram)
`NOT, !`	ist der Vergleichsoperator für die logische Negation. Der negierte Ausdruck ergibt „true“, wenn der benutzerdefinierte Ausdruck „false“ ist und „false“, wenn der benutzerdefinierte Ausdruck „true“ ist[c].
`OR, ||`	ist der logische Operator OR oder ||, die äquivalent sind[c].
`AND, &&`	ist der logische Operator AND oder &&, die äquivalent sind[c].
`customExpr`	ist ein in der Syntax für benutzerdefinierte Ausdrücke geschriebener Ausdruck (siehe oben)

a. Zum Schreiben eines benutzerdefinierten Ausdrucks in einem Protokollabfragefeld müssen Sie Systemprotokollvariablen verwenden. Zu diesen Variablen sind Onlinebeschreibungen verfügbar. Klicken Sie hierfür auf der Seite **New Filter** auf die Schaltfläche **?** (System > Log/Monitoring > Events | User Access | Admin Access > Registerkarte „Filters“).

b. Tag- und Zeitvergleiche werden in der Zeitzone des IVE ausgewertet. Berechnungen der Tagesbereiche (Tag **TO** Tag) beginnen mit dem ersten angegebenen Tag und werden schrittweise ausgeführt, bis der zweite angegebene Tag erreicht wird. In Berechnungen für Zeitbereiche (time **TO** time) muss der erste Wert zeitlich vor dem zweiten Wert liegen. Nur Zeitvariablen können mit Tages- und Zeitwerten verglichen werden. Zeitvariablen sind: `time.*` und `loginTime.*`

c. Die Operatoren NOT, AND und OR werden von der höchsten zur niedrigsten Priorität in folgender Rangfolge ausgewertet: NOT (von rechts), AND (von links), OR (von links)

Platzhalterabgleich

In einer Zeichenfolge, die in Anführungszeichen eingeschlossen ist, können Platzhalter verwendet werden. Folgende Platzhalter werden unterstützt:

- **Sternchen (*)**

  Ein Sternchen steht für eine beliebige Folge von null oder mehr Zeichen.

- **Fragezeichen (?)**

  Ein Fragezeichen steht für ein einzelnes Zeichen.

- **Eckige Klammern ([ ])**

  Eckige Klammern stehen für ein Zeichen aus einem Bereich möglicher Zeichen, der zwischen den Klammern angegeben wird. Zwei durch einen Bindestrich (-) getrennten Zeichen stehen für die beiden Zeichen und die lexikalisch dazwischen liegenden Zeichen. Beispiel: 'dept[0-9]' steht anstelle der Zeichenfolgen „dept0“, „dept1“ usw. bis einschließlich „dept9“.

Die Escape-Zeichen für Platzhalter sind eckige Klammern. So ergibt der Ausdruck ' userAttr.x = "value[*]" ' beispielsweise „true“, wenn das Attribut x genau gleich „value*“ ist.

DN-Variablen

Sie können einen Distinguished Name (DN) mit einem anderen DN oder einer Zeichenfolge vergleichen, Platzhalter werden dabei jedoch ignoriert. Bei Vergleichen wird die Groß- und Kleinschreibung nicht berücksichtigt, Leerzeichen werden ignoriert, und die Reihenfolge der Variablen wird berücksichtigt.

Wenn ein Ausdruck einen DN mit einer Zeichenfolge vergleicht, wird diese vor der Auswertung des Ausdrucks in einen DN konvertiert. Wenn die Zeichenfolge (aufgrund fehlerhafter Syntax) nicht konvertiert werden kann, schlägt der Vergleich fehl. DN-Variablen sind:

- userDN
- certDN
- certIssuerDN

Systemvariablen und Beispiele

Hinweis: Diese Liste enthält keine Variablen, die in einer Filterabfrage oder einem Exportformat für ein Systemprotokoll verwendet werden.

Variablen	Beschreibung	Beispiele
auth Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Name des Authentifizierungsservers, der einen Benutzer authentifiziert.	auth = MyLDAPServer
cacheCleaner Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Status der Cachebereinigung. Mögliche Werte: 1 – wenn sie ausgeführt wird 0 – wenn sie nicht ausgeführt wird	cacheCleanerStatus = 1 cacheCleanerStatus = 0
certAttr.<*cert-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • LDAP-Konfiguration • Felder für SSO-Parameter	Attribute aus einem clientseitigen Zertifikat. *cert-attr* kann einen der folgenden Werte annehmen: C, ST, L, O, OU, CN, T, I, G, S, D, SN, UI oder Email. Mithilfe dieser Variable können Sie überprüfen, ob der Client des Benutzers über ein clientseitiges Zertifikat mit den angegebenen Werten verfügt.	certAttr.OU = 'Retail Products Group'

CertAttr.altName.<*Alt-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • LDAP-Konfiguration • Felder für SSO-Parameter	Wert des alternativen Namens des Subjekts aus einem clientseitigen Zertifikat, wobei <*Alt-attr*> folgende Werte annehmen kann: .Email .directoryName .DNS .URI .ipAddress .registeredId	certAttr.altName.email = ‚joe@company.com‘ certAttr.altName.directoryName = „cn=joe, ou=company, o=com“ certAttr.altName.ipAddress = 10.10.83.2
certAttr.SN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • LDAP-Konfiguration • Felder für SSO-Parameter	Seriennummer eines Clientzertifikats. Beachten Sie, dass alle Zeichen außer [0-9 a-f A-F] aus einer Zeichenfolge vor dem Vergleich mit certAttr.SN entfernt werden. Platzhalter werden nicht unterstützt.	certAttr.SN = userAttr.certSerial certAttr.SN = „6f:05:45:ab“
certDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	DN des Clientzertifikat-Subjekts.	certDN = 'cn=John Harding,ou=eng,c=Company' certDN = userDN *(DN des Zertifikat-Subjekts wird mit dem DN des LDAP-Benutzers abgeglichen)* certDN = userAttr.x509SubjectName certDN = ('cn=John Harding,ou=eng,c=Company' or 'cn=Julia Yount,ou=eng,c=Company')
certDN.<*subject-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • LDAP-Konfiguration • Felder für SSO-Parameter	Beliebige Variable aus dem DN des Clientzertifikat-Subjekts, wobei *subject-attr* der Name des RDN-Schlüssels ist. Kann zum Testen verschiedener DN-Attribute in einem Standard-x.509-Zertifikat verwendet werden.	certDN.OU = ‚company‘ certDN.E = ‚joe@company.com‘ certDN.ST = ‚CA‘

certDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN eines Clientzertifikats. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	certDNText = 'cn=John Harding,ou=eng,c=Company'
certIssuerDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Subjekt-DN des Clientzertifikat-Ausstellers. Diese Variable verhält sich wie ein Standard-DN-Attribut (wie z. B. CertDN).	certIssuerDN = 'cn=John Harding,ou=eng,c=Company' certIssuerDN = userAttr.x509Issuer certIssuerDN = ('ou=eng,c=Company' or 'ou=operations,c=Company')
certIssuerDN.<*issuer-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Beliebige Variable aus dem Subjekt-DN des Clientzertifikat-Ausstellers, wobei *issuer-attr* der Name des RDN-Schlüssels ist.	certIssuerDN.OU = ‚company‘ certDN.ST = ‚CA‘
certIssuerDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Subjekt-DN des Clientzertifikat-Ausstellers. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	userDN = 'cn=John Harding,ou=eng,c=Company'

group.*<group-name>* Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln **Wichtig:** Nur für Rollenzuordnung ausgewertete Gruppen sind in den detaillierten Rollen (Bedingungen) in den Ressourcenrichtlinien verfügbar. Auch wenn der Benutzer einer Rolle mit einer ‚Stop'-Regel zugeordnet wird, werden Gruppen von nachfolgenden Regeln nicht zum Sitzungskontext des Benutzers hinzugefügt.	Sowohl statische als auch dynamische LDAP-Benutzergruppen, wobei group-name der im Wörterbuch angegebene Name der LDAP-Gruppe ist.	group.preferredPartner group.goldPartner or group.silverPartner group.employees and time.month = 9 ***Beispiele für Kombinationen:*** *Erlaubt alle Partner mit dem Status "Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'
hostCheckerPolicy Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Vom Client erfüllte Host Checker-Richtlinien.	hostCheckerPolicy = ('Norton' and 'Sygate') and cacheCleanerStatus = 1
loginTime Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Die Uhrzeit, zu der der Benutzer seine Anmeldeinformationen an das IVE sendet. Die Zeit basiert auf der IVE-Zeit. Hinweis: Bei Verwendung dieser Variable in einem SSO-Parameterfeld gibt die Variable die UNIX string time (Zeichenfolge, die die Uhrzeit enthält) zurück.	loginTime = (8:00am to 5:00pm) loginTime= (Mon to Fri)
loginTime.day Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der numerische Tag, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „day" einen Wert von 1-31 annehmen kann. Die Zeit basiert auf der IVE-Zeit.	loginTime.day = 3

loginTime.dayOfWeek Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der numerische Wochentag, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet. „dayOfWeek“ kann auf [0-6] gesetzt werden (0 = Sonntag).	loginTime.dayOfWeek != (0 OR 6)
loginTime.dayOfYear Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der numerische Tag des Jahres, an dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „dayOfYear“ auf [0-365] gesetzt werden kann.	loginTime.dayOfYear = 100
loginTime.month Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Monat, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „month“ auf [1-12] gesetzt werden kann (1 = Januar).	loginTime.month >= 4 AND loginTime.month <=9
loginTime.year Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Das Jahr, in dem der Benutzer seine Anmeldeinformationen an das IVE sendet, wobei „year“ auf [1900-2999] gesetzt werden kann.	loginTime.year = 2005
networkIf Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Die Netzwerkschnittstelle, an der eine Benutzerabfrage empfangen wird. Mögliche Werte: „internal“ oder „external“	sourceIp = 192.168.1.0/24 and networkIf = 'internal'

realm Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Der Name des Authentifzierungsbereichs, an dem der Benutzer angemeldet ist.	Realm = (‚GoldPartners‘ or ‚SilverPartners‘) ***Hinweis:*** *Die Bedingung AND führt zu keinem Ergebnis, da sich ein Benutzer in einer Sitzung nur an einem einzigen Bereich anmelden kann.*
resource Verfügbar in: Ressourcenrichtlinienregeln	Ressource, auf die ein Benutzer zuzugreifen versucht.	Resource = ‚www.yahoo.com‘
role Verfügbar in: • Ressourcenrichtlinienregeln • SSO	Liste aller Benutzerrollen für eine Sitzung. Wenn Sie in SSO alle Rollen an Back-End-Anwendungen senden möchten, verwenden Sie <role *sep* = ";"> – wobei *sep* die Zeichenfolge zum Trennen mehrerer Werte ist.	Role = (‚sales‘ or ‚engineering‘) Role = (‚Sales‘ AND ‚Support‘)
sourceIp Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Die IP-Adresse des Geräts, auf dem sich der Benutzer authentifiziert. Hinweis: In der Ressourcen-richtlinie kann die Netzmaske mit der Bitzahl oder im Netz-maskenformat ‚255.255.0.0‘ angegeben werden.	sourceIp = 192.168.10.20 sourceIp = 192.168.10.0/24 *(Klasse A)* sourceIp = 192.168.1.0/24 and networkIf = 'internal' userAttr.dept = ('eng' or 'it') and sourceIp = 10.11.0.0/16

time Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln HINWEIS: Fügen Sie für time.day eine separate Zeile ein, ähnlich wie bei loginTime.day.	Die Uhrzeit, zu der die Rollenzuordnungsregel oder die Ressourcenrichtlinienregel ausgewertet wird. Die Uhrzeit kann im 12- oder 24-Stunden-Format angegeben werden.	time = (9:00am to 5:00pm) time = (09:00 to 17:00) time = (Mon to Fri) ***Beispiele für Kombinationen:*** *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)
time.day Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Die Uhrzeit, zu der der Benutzer seine Anmeldeinformationen an das IVE sendet. Die Uhrzeit kann im 12- oder 24-Stunden-Format angegeben werden.	time.day = (9:00am to 5:00pm) time.day = (09:00 to 17:00) time.day = (Mon to Fri)
time.dayOfWeek Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Wochentag, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: Mon, Tue, Wed, Thu, Fri, Sat, Sun	time.dayOfweek = (Mon to Fri) time = (mon to fri) and time = (9:00am to 5:00pm) time = (sat to sun) and time = (8:00 to 23:00)
time.dayOfYear Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Tag im Jahr, an dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-365.	time.dayOfYear = 100

time.month Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Monat, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. Mögliche Werte sind: 1-12	time.month >= 9 and time.month <= 12 and time.year = 2004 group.employees and time.month = 9
time.year Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Das Jahr, in dem die Rollenzuordnungsregel oder Ressourcenrichtlinienregel ausgewertet wird. „year“ kann auf [1900-2999] gesetzt werden	time.year = 2005
user Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	IVE-Benutzername. Wenn sich der Benutzer an einem Zertifikat-Authentifizierungsserver anmeldet, ist sein IVE-Benutzername derselbe wie CertDN.cn.	user = 'steve' and time = mon user = 'steve' user = 'steve*' user = ('steve' or '*jankowski')
userAgent Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Die Benutzer-Agent-Zeichenfolge des Browsers.	userAgent = ‘*MSIE*’

userAttr.<*auth-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter **Wichtig:** Nur die für Rollenzuordnungsregeln ausgewerteten Attribute sind in den detaillierten Rollen (Bedingungen) in den Ressourcenrichtlinien verfügbar. Auch wenn der Benutzer einer Rolle mit einer ‚Stop'-Regel zugeordnet wird, werden Attribute von nachfolgenden Regeln nicht zum Sitzungskontext des Benutzers hinzugefügt.	Von einem LDAP- oder RADIUS-Server abgerufene Benutzerattribute.	userAttr.building = ('HQ*' or 'MtView[1-3]') userAttr.dept = ('sales' and 'eng') userAttr.dept = ('eng' or 'it' or 'custsupport') userAttr.division = 'sales' userAttr.employeeType != 'contractor' userAttr.salaryGrade > 10 userAttr.salesConfirmed >= userAttr.salesQuota ***Negative Beispiele:*** userAttr.company != "Acme Inc" or not group.contractors not (user = 'guest' or group.demo) ***Beispiele für Kombinationen:*** *Erlaubt leitenden Angestellten und deren Assistenten den Zugriff von Montag bis Freitag:* userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri) *Erlaubt alle Partner mit dem Status "Aktiv" von Montag bis Freitag, jedoch bevorzugte Partner von Montag bis Samstag:* ((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'

userDN Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln	Der Benutzer-DN von einem LDAP-Server. Wenn der Benutzer durch den LDAP-Server authentifiziert wird, stammt dieser DN vom Authentifizierungsserver, andernfalls stammt der DN vom Verzeichnis-/Attributserver des Bereichs.	userDN = 'cn=John Harding,ou=eng,c=Company'
userDN.<*user-attr*> Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Beliebige Variable aus dem Benutzer-DN, wobei *user-attr* der Name des RDN-Schlüssels ist.	userDN.ou = 'eng'
userDNText Verfügbar in: • Rollenzuordnungsregeln • Ressourcenrichtlinienregeln • Felder für SSO-Parameter	Als Zeichenfolge gespeicherter Benutzer-DN. Es sind nur Zeichenfolgenvergleiche mit diesem Wert zulässig.	userDNText = 'cn=John Harding,ou=eng,c=Company'

Appendix D.

Verwenden der seriellen Konsole des IVE

Die serielle Konsole des IVE bietet eine Oberfläche zum Durchführen der folgenden Vorgänge:

Herstellen einer Verbindung mit der seriellen Konsole des IVE 453
Rollback zu einem vorherigen Systemzustand 454
Zurücksetzen des IVE-Geräts auf die Werkseinstellungen 456
Durchführen gängiger Wiederherstellungsvorgänge 458
Erstellen weiterer Administratorkarten (nur Access Series FIPS) 460
Erstellen einer neuen Security World (nur Access Series FIPS) 461
Wiederherstellen einer archivierten Security World (nur Access Series FIPS) ... 463

☑ Herstellen einer Verbindung mit der seriellen Konsole des IVE

Um Aufgaben über die serielle Konsole des IVE durchführen zu können, müssen Sie eine Terminalkonsole oder einen Laptop an das IVE-Gerät anschließen.

So stellen Sie eine Verbindung mit der seriellen Konsole des IVE her:

1. Schließen Sie ein Nullmodem-Crossover-Kabel vom Konsolenterminal oder Laptop an das IVE-Gerät an. Dieses Kabel ist im Lieferumfang des Geräts enthalten. Verwenden Sie kein einfaches serielles Kabel.
2. Konfigurieren Sie das Terminal oder die Terminalemulationssoftware (beispielsweise HyperTerminal) mit den folgenden Parametern für serielle Verbindungen:
   - 9600 Bit pro Sekunde
   - 8 Bit, keine Parität (8N1)
   - 1 Stopp-Bit
   - Keine Flusskontrolle
3. Drücken Sie die **Eingabetaste**, bis die serielle Konsole von IVE angezeigt wird.

Hinweis: Wenn Sie ein Access Series FIPS-Gerät betreiben und zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen, müssen Sie zudem den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus) stellen.

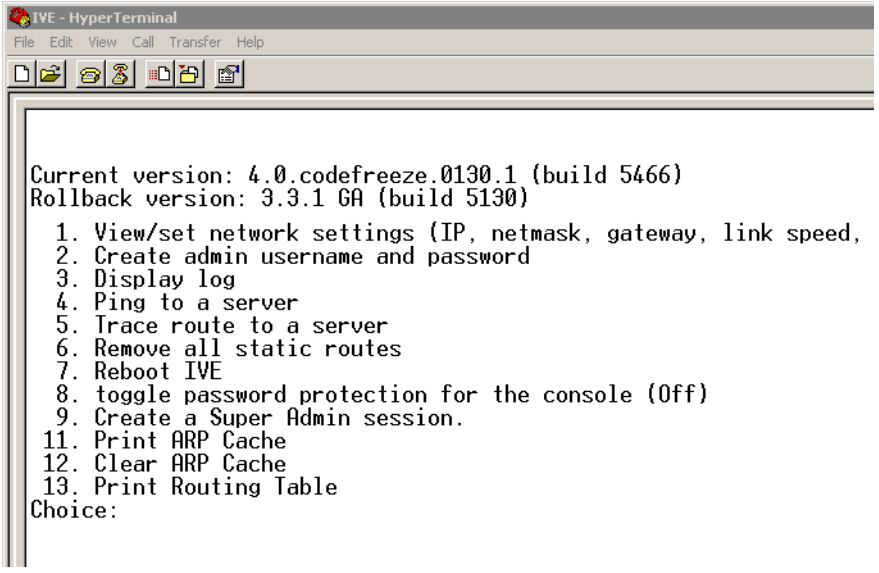

IVE - HyperTerminal
File Edit View Call Transfer Help
Current version: 4.0.codefreeze.0130.1 (build 5466)
Rollback version: 3.3.1 GA (build 5130)
1. View/set network settings (IP, netmask, gateway, link speed,
2. Create admin username and password
3. Display log
4. Ping to a server
5. Trace route to a server
6. Remove all static routes
7. Reboot IVE
8. toggle password protection for the console (Off)
9. Create a Super Admin session.
11. Print ARP Cache
12. Clear ARP Cache
13. Print Routing Table
Choice:

Abbildung 131:IVE Serielle Konsole

☑ Rollback zu einem vorherigen Systemzustand

Sie können das IVE-System normalerweise über die Webkonsole folgendermaßen in einen vorherigen Systemzustand zurückversetzen:

1. Navigieren Sie zu den zuvor gespeicherten System- und Benutzerkonfigurationsdateien, in denen die gewünschten Daten gespeichert sind.
2. Laden Sie die gewünschten Serverpakete unter „support.netscreen.com" herunter.
3. Importieren Sie das gewünschte Serverpaket.
4. Importieren Sie die gewünschten System- und Benutzerkonfigurationsdateien.

   Das IVE speichert die aktuellen Systemkonfigurationsinformationen und die des vorherigen Systemzustands. Wenn Sie das Serverpaket aktualisieren und Ihr Gerät in den vorherigen Zustand zurücksetzen möchten, empfehlen wir Ihnen, den zuvor aufgeführten Anweisungen zu folgen. Wenn Sie nicht auf die Webkonsole zugreifen können, stellen Sie eine Verbindung mit der seriellen Konsole her, um ein Rollback zum vorherigen Systemzustand durchzuführen.

   Wenn Sie bisher noch keine Serveraktualisierung durchgeführt haben, gibt es keinen älteren Systemzustand, und die Option ist daher nicht verfügbar. Wenn Sie eine Serveraktualisierung durchgeführt haben, gehen

alle System- und Benutzerkonfigurationsdaten, die nach der Aktualisierung erstellt wurden, verloren. Dies vermeiden Sie, indem Sie die aktuellen Konfigurationsdateien vor dem Rollback des Systems exportieren und anschließend wieder importieren.

Ein Rollback zu einem vorherigen Systemzustand ist auch über die Webkonsole möglich, wie unter „Installieren eines NetScreen-Softwaredienstpakets“ auf Seite 385 beschrieben.

Hinweis: Wenn Sie ein Access Series FIPS-Gerät betrieben und ein Rollback zu einer vorherigen Security World vornehmen möchten, folgen Sie den Anweisungen unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 463.

So führen Sie ein Rollback zum vorherigen Serverzustand durch:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 453).
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.
3. Wählen Sie **Maintenance > System > Platform** aus.
4. Klicken Sie auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.
5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie `rollback` ein, und drücken Sie dann die **Eingabetaste**.

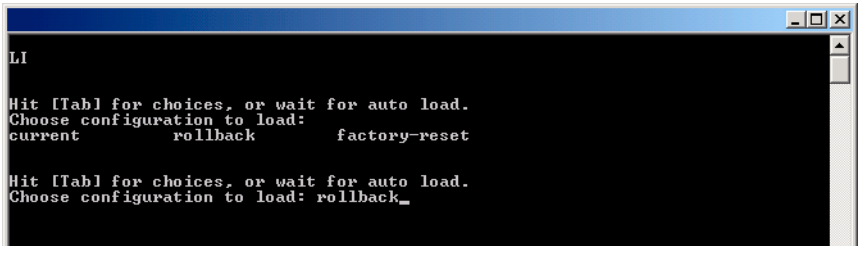

LI
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current rollback factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: rollback

Abbildung 132:IVE Serielle Konsole
Nach dem Klicken auf „Reboot Now“ auf der Seite Maintenance > System > Platform.

Hinweis:

- Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Webkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.
- Wenn Sie bereits ein Systemrollback durchgeführt haben, ist die Rollbackoption erst wieder verfügbar, wenn Sie die Serversoftware erneut aktualisieren.

Der Rollbackstatus des Servers wird auf den Bildschirm ausgegeben. Wenn der Vorgang abgeschlossen ist, werden Sie zum Drücken der **Eingabetaste** aufgefordert, um die Systemeinstellungen zu ändern. Dadurch kehren Sie zu den Optionen für das erste Setup zurück. Wenn Sie die Dateneingabe abgeschlossen haben, schließen Sie einfach das Programmfenster.

☑ Zurücksetzen des IVE-Geräts auf die Werkseinstellungen

Es kann im Ausnahmefall erforderlich sein, das IVE-Gerät auf die Werkseinstellungen zurückzusetzen. Bevor Sie diese tief greifende Systemwiederherstellungsoption ausführen, wenden Sie sich bitte unter der Adresse „help@support.netscreen.com“ an den NetScreen-Support. Vor dem Zurücksetzen auf die Werkseinstellungen sollten Sie nach Möglichkeit die aktuellen System- und Benutzerkonfigurationsdaten exportieren.

So setzen Sie das Gerät auf die Werkseinstellungen zurück:

1. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 453).
2. Melden Sie sich in einem Browserfenster an der Webkonsole an.
3. Wählen Sie **Maintenance > System > Platform** aus.
4. Klicken Sie auf **Reboot Now**, und wechseln Sie dann wieder zum Konsolenprogrammfenster zurück. Im Fenster werden Sie in einer Meldung informiert, dass das System neu gestartet wird.
5. Nach kurzer Zeit werden Sie aufgefordert, für die Auswahl von Optionen die **Tab-Taste** zu drücken. Drücken Sie die **Tab-Taste**. Wenn Sie gefragt werden, welche Konfiguration geladen werden soll, geben Sie `factory-reset` ein, und drücken Sie dann die **Eingabetaste**.

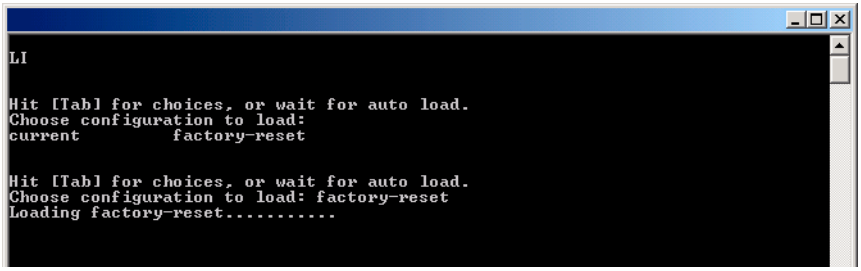

LI
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load:
current factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: factory-reset
Loading factory-reset.....

Abbildung 133:IVE Serielle Konsole
Nach dem Klicken auf „Reboot Now" auf der Seite Maintenance > System > Platform.

Hinweis: Wenn Sie beim Auswählen länger als 5 Sekunden warten, wird automatisch die aktuelle Systemkonfiguration geladen. Sie müssen dann zurück in die Webkonsole wechseln und auf **Reboot Now** klicken, um den Vorgang erneut zu starten.

---

6. Wenn Sie aufgefordert werden, das Zurücksetzen auf die Werkseinstellungen zu bestätigen, geben Sie `proceed` ein, und drücken Sie dann die **Eingabetaste**.

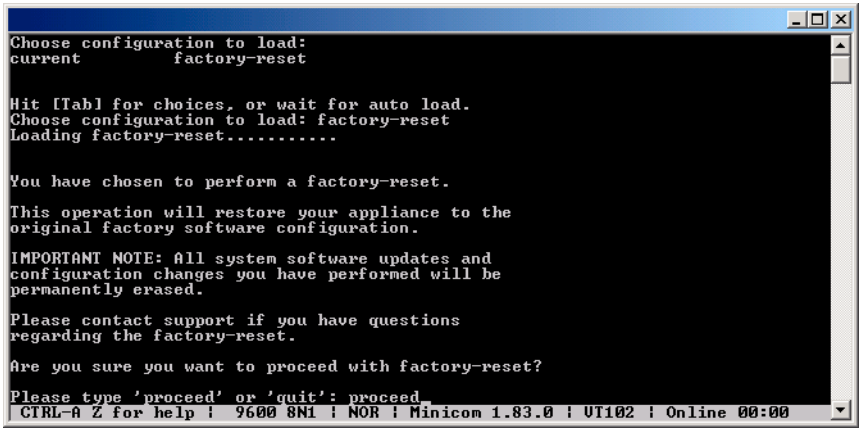

Choose configuration to load:
current factory-reset
Hit [Tab] for choices, or wait for auto load.
Choose configuration to load: factory-reset
Loading factory-reset.....
You have chosen to perform a factory-reset.
This operation will restore your appliance to the
original factory software configuration.
IMPORTANT NOTE: All system software updates and
configuration changes you have performed will be
permanently erased.
Please contact support if you have questions
regarding the factory-reset.
Are you sure you want to proceed with factory-reset?
Please type 'proceed' or 'quit': proceed
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 1.83.0 | VT102 | Online 00:00

Abbildung 134:IVE Serielle Konsole
Hier wurde das Zurücksetzen auf die Werkseinstellungen ausgewählt.

Das System beginnt mit dem Zurücksetzen des Geräts auf die Originaleinstellungen und gibt dabei mehrere Bildschirme mit Daten aus. Nach einigen Minuten werden Sie aufgefordert, für die Auswahl von Konfigurationsoptionen die **Tab-Taste** zu drücken.

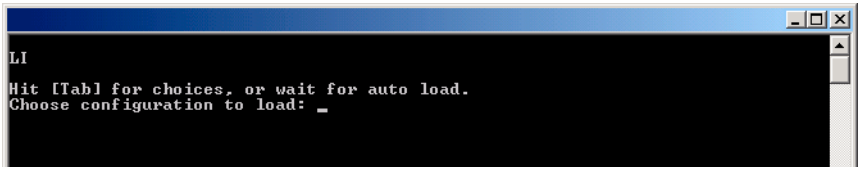


Abbildung 135:IVE Serielle Konsole
Nach dem Zurücksetzen auf die Werkseinstellungen.

7. Wenn Sie zum Drücken der **Tab-Taste** aufgefordert werden, gibt es folgende Möglichkeiten:
   - Warten Sie den automatischen Start der Standardoption ab (`current`), oder
   - drücken Sie die **Tab-Taste**, geben Sie `current` ein, und drücken Sie dann die **Eingabetaste**.

   Sie werden dann aufgefordert, die ursprünglichen Konfigurationseinstellungen des Geräts einzugeben. Detaillierte Informationen zur Vorgehensweise können Sie dem Installationshandbuch entnehmen, das dem Gerät beiliegt. Dieses Handbuch steht auch auf der NetScreen-Supportsite im PDF-Format zur Verfügung.

   Nach dem Abschluss des Initialisierungsvorgangs können Sie auf das neueste Serverpaket aktualisieren und die gespeicherten System- und Benutzerkonfigurationsdateien importieren, um zum letzten funktionstüchtigen Zustand des Geräts zurückzukehren.

☑ Durchführen gängiger Wiederherstellungsvorgänge

Wenn Sie den Administratorbenutzernamen und/oder das Administratorkennwort für das IVE vergessen, sich aufgrund von Konfigurationsfehlern selbst vom Gerät ausgesperrt oder die IP-Adresse des IVE-Geräts geändert haben und nicht mehr auf das Gerät zugreifen können, können Sie die Geräteeinstellungen über die serielle Konsole ändern. Folgen Sie den Anweisungen unter „Herstellen einer Verbindung mit der seriellen Konsole des IVE“ auf Seite 453, und wählen Sie dann den gewünschten Konfigurationsvorgang aus.

- **Anzeigen/Festlegen der Netzwerkeinstellungen**

  Hiermit können Sie die Standardnetzwerkeinstellungen ändern.

- **Erstellen von Administratorbenutzername und -kennwort**

  Hiermit können Sie ein neues Super-Administratorkonto anlegen.

- **Anzeigen der Systemprotokolle**

  Hiermit können Sie die Systemkonfiguration, Benutzerprotokolle oder Protokolle des Administratorzugriffs über die serielle Konsole anzeigen. Nach dem Anzeigen der Protokolle müssen Sie „q" eingeben, um wieder die Optionen der seriellen Konsole anzuzeigen.

- **Aktivieren/Deaktivieren des Kennwortschutzes**

  Hiermit können Sie die Konsole durch ein Kennwort sichern. Wenn Sie diese Option auf „on" setzen, ist der Zugriff nur Super-Administratoren gestattet.

- **Erstellen einer Super-Administratorsitzung**

  Hiermit können Sie eine Wiederherstellungssitzung auf der Webkonsole erstellen, auch wenn der Administratorzugriff auf das IVE gesperrt ist. Wenn Sie diese Option aktivieren, generiert das IVE einen temporären Token, der drei Minuten gültig ist. Geben Sie den folgenden URL in ein Browserfenster ein: `https://<ive-host>/dana-na/auth/recover.cgi`. Geben Sie dann bei der entsprechenden Aufforderung den temporären Token ein, um sich an der Webkonsole anzumelden.

- **Testen der Verbindung und Konfiguration weiterer Netzwerkeinstellungen**

  Hiermit können Sie einen Ping-Befehl auf einen anderen Server ausführen, die Route zu einem Server verfolgen, statische Routen entfernen, den ARP-Cache ausgeben, den ARP-Cache leeren und eine Routingtabelle ausgeben.

Hinweis: Wenn Sie ein Access Series FIPS-System ausführen und im Kryptographiemodul den Löschschalter gedrückt haben, stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), und starten Sie das System neu. Zum Wiederherstellen benötigen Sie keinen Zugriff auf die serielle Konsole.

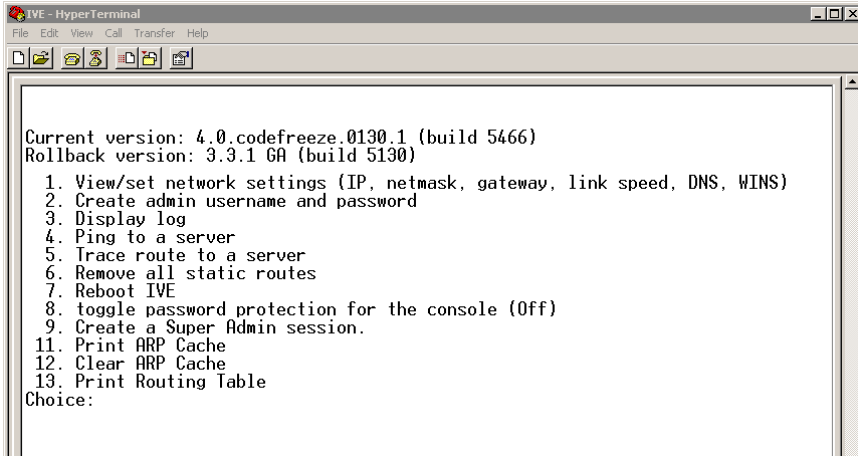

IVE - HyperTerminal
File Edit View Call Transfer Help
Current version: 4.0.codefreeze.0130.1 (build 5466)
Rollback version: 3.3.1 GA (build 5130)
1. View/set network settings (IP, netmask, gateway, link speed, DNS, WINS)
2. Create admin username and password
3. Display log
4. Ping to a server
5. Trace route to a server
6. Remove all static routes
7. Reboot IVE
8. toggle password protection for the console (Off)
9. Create a Super Admin session.
11. Print ARP Cache
12. Clear ARP Cache
13. Print Routing Table
Choice:

Abbildung 136:IVE Serielle Konsole
Systempflege

☑ Erstellen weiterer Administratorkarten (nur Access Series FIPS)

Um für eine Security World weitere Administratorkarten erstellen zu können, müssen Sie über Folgendes verfügen:

- Ein Kryptographiemodul, das zur Security World gehört
- Einen Smartcardleser
- Eine Administratorkarte, die mit der Security World vorinitialisiert ist
- Eine oder mehrere unformatierte Smartcards oder Administratorkarten mit Daten, die Sie gefahrlos überschreiben können

Hinweis: Wenn Sie zusätzliche Smartcards benötigen, wenden Sie sich an Ihren IVE-Händler.

So erstellen Sie weitere Administratorkarten für eine Security World:

1. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport eines Kryptographiemoduls an, das zur Security World gehört. Der Port befindet sich an der Frontplatte des IVE-Geräts.
2. Legen Sie eine vorinitialisierte Administratorkarte für die Security World mit den Kontakten nach oben in den Smartcardleser ein.

3. Stellen Sie den Modusschalter des Kryptographiemoduls auf **O** (Operationsmodus), sofern dieser sich nicht bereits in dieser Position befindet.
4. Stellen Sie eine Verbindung mit der seriellen Konsole her (Seite 453).
5. Wählen Sie in der Liste der Konfigurationsaufgaben den Eintrag **Replace Administrator Card Set** aus.
6. Geben Sie das Kennwort für die Security World ein.
7. Legen Sie nach der entsprechenden Aufforderung eine unformatierte Smartcard oder eine Administratorkarte, deren Daten Sie gefahrlos überschreiben können , mit den Kontakten nach oben in den Smartcardleser ein.
8. Geben Sie die angeforderten zusätzlichen Initialisierungsinformationen ein.
9. Wiederholen Sie Schritt 7 für alle weiteren Karten, die Sie erstellen möchten.
10. Verwahren Sie mindestens eine der Administratorkarten an einem sicheren Ort.

☑ Erstellen einer neuen Security World (nur Access Series FIPS)

Sie können ein Access Series FIPS-Gerät erst verwenden, wenn Sie für dieses eine Security World erstellt haben. In manchen Fällen müssen Sie jedoch eine Security World mit einer neuen überschreiben. Wenn Sie z. B. eine Administratorkarte verlieren, sollten Sie eine völlig neue Security World erstellen, um zu verhindern, dass eine nicht vertrauenswürdige Person die Karte findet und auf Ihre Security World zugreifen kann. Auch wenn Sie das Kennwort für die ursprüngliche Security World vergessen haben, müssen Sie eine neue Security World erstellen.

Um eine neue Security World erstellen zu können, müssen Sie über Folgendes verfügen:

- Die Kryptographiemodule, die zur Security World gehören
- Einen Smartcardleser
- Eine oder mehrere unformatierte Smartcards oder Administratorkarten mit Daten, die Sie gefahrlos überschreiben können

---

Hinweis: Die alten Administratorkarten können für die neue Security World nur verwendet werden, wenn Sie sie mit den Daten der neuen Security World neu formatieren.

Informationen zum Überschreiben einer Security World mit einer vorhandenen Security World finden Sie unter „Wiederherstellen einer archivierten Security World (nur Access Series FIPS)“ auf Seite 463.

So erstellen Sie eine neue Security World für ein eigenständiges IVE:

1. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
2. Legen Sie eine unformatierte Smartcard oder eine Administratorkarte mit Daten, die Sie gefahrlos überschreiben können , mit den Kontakten nach oben in den Smartcardleser ein.
3. Stellen Sie den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus).
4. Greifen Sie auf die serielle Konsole des IVE zu, und starten Sie das IVE (Seite 453) neu.
5. Geben Sie die angeforderten Initialisierungsinformationen ein.
6. Stellen Sie den Modusschalter des Kryptographiemoduls auf O (Operationsmodus) zurück, wenn Sie dazu aufgefordert werden.
7. Erstellen Sie ein neues Serverzertifikat, für das der neue private Schlüssel der Security World verwendet wird (Seite 151).

So erstellen Sie eine neue Security World in einer Clusterumgebung:

1. Melden Sie sich an der Webkonsole eines Clusterknotens an, den Sie mit einer neuen Security World neu formatieren möchten. Um auf die Webkonsole eines Clusterknotens zuzugreifen, geben Sie in einem Browser seine interne IP-Adresse, gefolgt von „/admin", ein. Beispiel: https://x.x.x.x/admin
2. Aktivieren Sie auf der Registerkarte **System > Clustering > Status** in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Disable**.
3. Initialisieren Sie das Clustermitglied mit einer Security World. Gehen Sie folgendermaßen vor:
   - Wenn dies der erste Knoten im Cluster ist, erstellen Sie eine neue Security World (Seite 461).
   - Wenn dies ein nachfolgender Knoten im Cluster ist, initialisieren Sie das Gerät mit der vorhandenen Security World des Clusters (Seite 464).
4. Kehren Sie zur Registerkarte **System > Clustering > Status** des Knotens zurück, aktivieren Sie in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Enable**.
5. Führen Sie diese Schritte für jeden Knoten im Cluster durch.

☑ Wiederherstellen einer archivierten Security World (nur Access Series FIPS)

In seltenen Fällen müssen Sie das System mithilfe einer archivierten Security World wiederherstellen. Die archivierte Security World kann eine ältere Version als die im System vorhandene Security World sein oder mit dieser übereinstimmen. Um das System wiederherzustellen, müssen Sie auf die Systemkonfigurationsdatei (in der Standardeinstellung `system.cfg`) zugreifen können, die die archivierte Security World und das entsprechende Zertifikat enthält.

Wenn Sie ein Security World mit einer anderen Security World überschreiben, müssen Sie außerdem über Folgendes verfügen:

- Alle Kryptographiemodule, die zur Security World gehören
- Einen Smartcardleser
- Eine Administratorkarte, die mit der Security World und dem Administratorkennwort vorinitialisiert ist, die Sie importieren möchten

So importieren Sie eine vorhandene Security World in ein eigenständiges IVE:

1. Importieren Sie die Systemkonfigurationsdatei, die die archivierte Security World und das entsprechende Zertifikat enthält, in das IVE(Seite 389), und initialisieren Sie ggf. die Security World. Enthält die Konfigurationsdatei eine archivierte Version von:
   - der Security World, die auf dem Computer bereits vorhanden war, ist keine weitere Konfiguration erforderlich.
   - einer anderen Security World als der, die auf dem Computer bereits vorhanden war, müssen Sie die neue Security World initialisieren.

   Hinweis: Wenn Sie eine Konfigurationsdatei importieren, die eine andere Security World enthält, können Sie Ihre vorhandenen Administratorkarten erst für die importierte Security World verwenden, wenn Sie sie mit den Daten der neuen Security World neu formatiert haben.
2. Schließen Sie das Kabel des Smartcardlesers an den Lesegerätport des Kryptographiemoduls an, der sich an der Frontplatte des IVE-Geräts befindet.
3. Legen Sie eine Administratorkarte, die mit der importierten Security World vorinitialisiert wurde, mit den Kontakten nach oben in den Smartcardleser ein.
4. Stellen Sie den Modusschalter des Kryptographiemoduls auf I (Initialisierungsmodus).

5. Greifen Sie auf die serielle Konsole des IVE zu, und starten Sie das IVE (Seite 453) neu.
6. Geben Sie die angeforderten Initialisierungsinformationen ein.
7. Stellen Sie den Modusschalter des Kryptographiemoduls auf O (Operationsmodus) zurück, wenn Sie dazu aufgefordert werden.

So importieren Sie eine vorhandene Security World in einen Cluster:

1. Melden Sie sich an der Webkonsole eines Clusterknotens an, den Sie mit einer neuen Security World neu formatieren möchten. Um auf die Webkonsole eines Clusterknotens zuzugreifen, geben Sie in einem Browser seine interne IP-Adresse, gefolgt von „/admin", ein. Beispiel: https://x.x.x.x/admin
2. Aktivieren Sie auf der Registerkarte **System > Clustering > Status** in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens, und klicken Sie dann auf **Disable**.
3. Importieren Sie eine archivierte Security World in das Clustermitglied (Seite 463).
4. Nach Abschluss des Installationsvorgangs kehren Sie zur Registerkarte **System > Clustering > Status** des Knotens zurück, aktivieren in der Spalte **Cluster Members** das Kontrollkästchen neben dem Namen des Knotens und klicken dann auf **Enable**.
5. Führen Sie diese Schritte für jeden Knoten im Cluster durch.

Index

Symbole

.Administratorrolle 268
.Read-Only Administratorrolle 268

Zahlen

128-Bit-Verschlüsselung 140
168-Bit-Verschlüsselung 140

A

Ablaufverfolgungsdatei (zur Fehlerbehebung) 413
AcceptTPCookie, Einstellung für Netegrity SiteMinder 250
Access Series FIPS
  Administratorkarte
    Beschreibung 10
    Erstellung 460
    Sicherheit 11
    Übersicht 11
    Verwaltung 11
  Clustering 81, 175
  Initialisierungsmodus 10
  Operationsmodus 10
  Security World
    Übersicht 9
    Verwaltung 11
  Security World-Schlüssel
    Definition 9
  Übersicht 9
  Wartungsmodus 10
  Wiederherstellungsvorgänge 459
  Zertifikate 70
Access Series, Definition 7
Access-Accept-Authentifizierung 243
Access-Challenge-Authentifizierung 243
Access-Reject-Authentifizierung 243
Access-Request-Authentifizierung 243
ACE siehe RSA ACE
Active Directory
  Siehe Authentifizierungsserver, Active Directory
ActiveX
  Aktivierung 19
  Anforderungen
    Cachebereinigung 64
    Hostprüfung 91
    Secure Meeting 19
Administrator
  Benutzeradministrator 213
  Rolle
    Definition 55
  Rollen
    Definition 83
    Konfiguration 265
  Rolle
    Siehe auch Rolle
AES-Verschlüsselung, Unterstützung 216
Aktion, Bestandteil einer Ressourcenrichtlinie 43
Aktiv/Aktiv-Cluster
  Abbildung 79
  Bereitstellung, Übersicht 78
Aktiv/Passiv-Cluster
  Abbildung 77
  Bereitstellung, Übersicht 76
Aktive Benutzer überwachen 131
Anmeldeinformationen
  an andere Anwendung senden 107
  Überprüfung 5
  Vermittlung 141
  Windows 355
Anmelderichtlinien
  Aktivierung 208
  Auswertung 206
  Deaktivierung 208
  Definition 6, 203
  Konfiguration 204
  Reihenfolge ändern 207
  vorkonfigurierte Richtlinien 6
Anmeldeseiten
  benutzerdefiniert 209
  Definition 209

Standard 209
Zuordnung zu Anmelderichtlinien 204
Anmeldung
Optionen
Benutzereinschränkungen 428, 429, 432, 433, 434, 435
anonymer Server
Siehe Authentifizierungsserver, anonymer Server
Anpassbare Oberfläche
mit SiteMinder verwenden 249
Anpassbare Oberfläche hochladen 209
Anwendungscaches leeren 63
Archiv
Definition 96
Planung 403
archiveFileTransferFailed, MIB-Objekt 198
archiveServerLoginFailed, MIB-Objekt 198
archiveServerUnreachable, MIB-Objekt 198
ARP Ping Timeout, Konfiguration 158, 161
ARP-Befehl 417, 458
Attribute konfigurieren 277
Attributserver
Siehe Authentifizierungsserver
Ausfallfreie Aktualisierung, Übersicht 67
Ausführung unter MS und SUN JVM 71
Authentifizierung
unterstützte Server 36
Authentifizierungsbereiche
Siehe Bereich
Authentifizierungseinstellungen
für Benutzer 428, 432, 433, 434, 435
Authentifizierungsrichtlinie
Konfiguration 275
Authentifizierungsrichtlinien
Definition 6, 23, 35
Konfiguration 36
Authentifizierungsschema, Definition 248
Authentifizierungsserver
ACE/Server
ACE/Agent-Datei generieren 219
Agent-Konfigurationsdatei 219
Konfiguration 217
SecurID-Authentifizierung 248
SecurID-Token 247
Übersicht 215
Active Directory
Konfiguration 213, 221
anonymer Server
Konfiguration 224, 263
Übersicht 223
Definition 5, 23, 35
Konfiguration (grundlegende Schritte) 212
LDAP
Attribute, Konfiguration 277
Beispiel 225
Konfiguration 213, 229
lokale Authentifizierung 235
Konfiguration 213, 263
NIS-Server
Konfiguration 241
RADIUS 243
ACE/Server-Protokoll 216
Attribute konfigurieren 277
SiteMinder 252, 255
Einzelanmeldung 250
Übersicht 247
unterstützte Versionen 248
Übersicht 212
vorkonfigurierte Server 5
Zertifikatserver
Definition 69
Konfiguration 225
zu Bereich zuordnen 274
Authentifizierungsvermittlung konfigurieren 140
Autorisierungsgruppe
Anmeldeeinschränkungen
über IP 428, 434, 435
über Zertifikat 432, 433
Lesezeichen
für das Web erstellen 295, 296, 299, 302, 312, 315, 316, 322
unter UNIX erstellen 301
Autorisierungsserver
Siehe Authentifizierungsserver

B

Basis-Authentifizierungsvermittlung
konfigurieren 140
Befehle, UNIX 417
Benachrichtigungs-E-Mails
Siehe Secure Meeting, Benachrichtigungs-E-Mails

Benutzer
'Benutzeradministratoren'
authentifizieren 213
Definition 238
Aktivität anzeigen 126
Anmeldeeinschränkungen
über Browser 429
über Zertifikat 432, 433
Anmeldeinformationen vermitteln 141
Attribute konfigurieren 277
Beenden erzwingen 132
clientseitiges Zertifikat erforderlich 70, 153
Codesignaturzertifikat für 71
Daten
Export 395
Import 397
Erstellung 236
Höchstanzahl 275
Konten
Export 393
Import 393
Kontoverwaltung 237
PCs konfigurieren 310, 311
Profildaten 80
Rolle
Definition 55
Sitzungen überwachen 131
Sitzungsdaten 80
Überwachung 131
Benutzerdefinierte Ausdrücke verwenden 278
Benutzer
Rolle
Siehe auch Rolle
Benutzerrolle
Siehe Rolle
Bereich
Definition 6, 23
Konfiguration 273, 427
Sicherheitsanforderungen 24
vorkonfigurierte Bereiche 6
Zuordnung zu Anmelderichtlinie 204
Beschleunigerkarte
SSL 387
ZIP 387
Broadcast-Synchronisierungsprotokoll 81
Browser
Anmeldeeinschränkungen, Benutzer 429
Cachesteuerung, Unterstützung 332
Einschränkungen konfigurieren 24, 25, 28
Richtlinien 429
Browsereinschränkungen konfigurieren 24
Browsingprobleme (Web) 413

C

Cache
Header 334
Java Plug-In 72
leeren 63
Regeln 332
Cachebereinigung
Einschränkungen konfigurieren 24, 25
Konfiguration 64, 146
Sicherheitsanforderungen festlegen 32
Übersicht 63
Cachesteuerung
No-Store 334
Central Manager, Übersicht 67
Chat-Fenster
Siehe Secure Meeting, Textnachrichten
Citrix NFuse
Liste unterstützter Versionen 120
Übersicht 120
Clientseitige Java-Applets
Verbindungen angeben 336, 337
Cluster
ACE/Server, Unterstützung 216
aktiv/aktiv 78
aktiv/passiv 76
Aktualisierung 173
Beitritt 175
Definition 168
Eigenschaften ändern 182
Erstellung 168
Hostnamen 158, 164
Initialisierung 76, 168
Kennwort 79
Konfiguration 75, 167
löschen 184
Protokollierung 80, 81
Status, Definition 173, 197
Statussynchronisierung 79
Synchronisierung 76, 79, 81
über serielle Konsole hinzufügen 179
über Webkonsole hinzufügen 176
Verwaltung 170, 172

Clusterpaar
Anforderungen 167
Definition 75
Codesignaturrichtlinien für Java 337
Codesignaturzertifikat
Siehe Zertifikat, Appletzertifikat
Codierung von Ressourcenrichtlinien 360
CPU-Nutzung, Anzeige 126
Critical (Protokollmeldung), Definition 96
CRL 5, 225
CyberGatekeeper
erzwingen 143
Integration 91

D

Dashboard
Konfiguration 125
Übersicht 67
Datei
Navigation konfigurieren 24
Ressourcenrichtlinien 42, 351
Definition 48, 49
Rollen konfigurieren 56
Server, Codierung 360
Zugriffsstatistik 200
Dateibereinigung 63
Datenbank für Authentifizierung 36
Datum und Uhrzeit einstellen 130
Delegierte Administration
Übersicht 83
Siehe auch Administratorrollen
DES/SDI-Verschlüsselung, Unterstützung 216
Detaillierte Regeln
Siehe Regeln
Diagramme, Konfiguration 125
Dienstpaket
herunterladen 129
Installation 385
Installation in einem Cluster 173
Digitales Zertifikat
Siehe Zertifikat
Distinguished Name-Attribute, Angabe 71
DMZ
Konfiguration 161
Schnittstelle 157, 161
DN-Attribute, Angabe 71
DNS
für externen Port 157, 161
für J-SAM konfigurieren 310
Hostname, Definition in Ressourcenrichtlinien 46, 50
Namensauflösung, Konfiguration 159
Durchgangsproxy
Anwendungen angeben für 339
Beschreibung 103
Ressourcenrichtlinien
Ressourcenrichtlinien Durchgangsproxy 340
Durchsatz, Anzeige 126

E

Einschränkungen
Benutzeranmeldung 432, 433
Einzelanmeldung
Siehe
Authentifizierungsserver, SiteMinder
Remote-SSO (Option)
E-Mail-Benachrichtigungen, Secure Meeting
Siehe Secure Meeting, Benachrichtigungs-E-Mails
E-Mail-Client
Konfiguration 24, 379
MIB-Objekt 197
Ressourcenrichtlinien 42, 379
Übersicht 85
Endpunktsicherheitsprüfung
Siehe Hostprüfung
Event Monitor, Anzeige 128
Exchange Server, Unterstützung 90
externalAuthServerUnreachable, MIB-Objekt 198
Externer Port, Konfiguration 161

F

Failover-Vorgänge 78
Federal Information Processing Standards
Siehe Access Series FIPS
Fehlerbehebung
Ablaufverfolgungsdatei 413
remote 418

Snapshotdatei 414
TCP-Dumpdatei 415
UNIX-Befehle 417
Fehlermeldungen ändern 209
FIPS
Siehe Access Series FIPS
Firewall
Unterstützung 91
Firewalls mit Cachebereinigung verwenden 64
Form-POST-Richtlinie, Übersicht 107
Freigabe
Definition in Ressourcenrichtlinien 48
FTP-Archiv, Definition 96

G

Gateway
für externen Port 157, 161
Konfiguration 158, 161
Gruppenmitgliedschaft, LDAP 278
Gültige Rollen, Definition 38, 58

H

Hardwaresicherheitsmodul
Siehe Access Series FIPS
Header/Cookies-Richtlinie, Übersicht 107
Hilfe ändern 209
Hilfe, an Support wenden ix
Host, Definition in Ressourcenrichtlinien 46, 50
Hostname
Auflösung 164
Definition in Ressourcenrichtlinien 46, 48, 49
Hostprüfung
API 91
Einschränkungen konfigurieren 24, 25
Konfiguration 143
Richtlinien 434, 435
Sicherheitsanforderungen festlegen 31
Übersicht 91
Hostzuordnung
für Client/Server-Anwendungen 314
HP OpenView, Unterstützung 96
HSM
Siehe Access Series FIPS

I

IMAP
Mailserver 379
Unterstützung 85, 87, 90
Info (Protokollmeldung), Definition 97
InfoExpress
erzwingen 143
Integration 91
Initialisierungsmodus, Access Series FIPS 10
Installation
Kontaktaufnahme mit Support, Hilfe ix
Instant Virtual Extranet
Siehe IVE
Interner Port, Konfiguration 157
Internet Explorer
Cachesteuerungs-Header, Unterstützung 332
Secure Meeting, Unterstützung 18
Siehe IE Explorer
Internet Explorer, JVM-Ausführung 72
Internet Mail Application Protocol, Unterstützung 85
Internet Explorer
JVM-Ausführung 72
IP-Adresse
Anmeldeeinschränkungen, Benutzer 428, 434, 435
Auflösung 164
Benutzeranforderungen angeben 26
Definition in Ressourcenrichtlinien 46, 47, 48, 49, 50
für externen Port 157, 161
Konfiguration 158, 161
Network Connect, Zuordnung 100
Pools, Ressourcenrichtlinien 51
Richtlinien 428
IVE
als SiteMinder-Webagent konfigurieren 252
Definition 3
Erstkonfiguration 7
herunterfahren 383
in LAN (Abbildung) 4
Konfiguration (grundlegende Schritte) 5
RADIUS für Erkennung konfigurieren 245
IVE neu starten, IVE herunterfahren
neu starten 383
IVE-Gäste
Siehe Secure Meeting, Rollen

iveLogFull, MIB-Objekt 197
iveLogNearlyFull, MIB-Objekt 197
iveMaxConcurrentUsersSignedIn, MIB-Objekt 197
iveReboot, MIB-Objekt 198
iveShutdown, MIB-Objekt 198
iveStart, MIB-Objekt 198
iveTooManyFailedLoginAttempts, MIB-Objekt 198

J

Java Plug-In, Cache 72
Java Virtual Machine
  Siehe JVM
Java-Applets
  Verbindungen angeben 336, 337
JavaScript
  Aktivierung 19
  Secure Meeting, Anforderungen 19
JavaSoft-Zertifikat 72
JVM
  Anforderungen
    J-SAM 119
    Secure Meeting 19
  Applet-Signierung 72
  mit nicht unterstützten Versionen arbeiten 104

K

Kalender *Siehe* Secure Meeting, Kalender
Kanonisches Format
  Übersicht 45
Kennwort
  Einschränkungen konfigurieren 24
  Richtlinien 433
  Sicherheitsanforderungen festlegen 30
Kennwortverwaltung
  Konfiguration 229
Knoten, Cluster 170, 172
Konferenzleiter
  Siehe Secure Meeting, Rollen
Konfiguration, Systemaktualisierung ix
Konfigurationsdatei
  ACLs und Lesezeichen exportieren 395
  ACLs und Lesezeichen importieren 397
  lokale Benutzerkonten exportieren 393
  lokale Benutzerkonten importieren 393
  System exportieren 389
  System importieren 390
  Übertragung 399
Konfigurationsübertragung 399
Konsole
  seriell
    Siehe Serielle Konsole
  Web
    Siehe Webkonsole
Kryptographiemodul
  Definition 9
  Siehe Access Series FIPS

L

L7-Überprüfungs-URL 78
LAN, Netzwerkeinstellungen ändern 157, 161
LDAP-Server
  Siehe Authentifizierungsserver, LDAP
Legacymodus
  Siehe 2.x-Autorisierungsmodus
Lesezeichen
  Export 395
  für das Web erstellen 295, 296, 299, 302, 312, 315, 316, 322
  Import 397
  Konfiguration 24
  unter UNIX erstellen 301
Linux, Unterstützung
  Secure Meeting 18
Linux-Unterstützung
  J-SAM 113
Lizenzen
  Aktualisierung 138
  Übersicht 137
Load-Balancer in einem Cluster verwenden 78
Localhost
  Hostnamenauflösung 113
  Remoteserver auflösen 112
logFullPercent, MIB-Objekt 197
Lokaler Authentifizierungsserver
  Siehe Authentifizierungsserver, lokale Authentifizierung
Lokaler IVE-Server
  Siehe Authentifizierungsserver, lokale Authentifizierung 235

Loopback-Adressen, J-SAM 111, 115
Lotus Notes
  Abbildung 120
  Übersicht 119
  Unterstützung 85, 90, 119

M

Macintosh
  Cachesteuerungs-Header, Unterstützung 332
Macintosh, Unterstützung
  Secure Meeting 18
Macintosh-Unterstützung
  J-SAM 113
Mail
  Server konfigurieren 379
  Spitzennutzungsstatistik 200
Major (Protokollmeldung), Definition 96
Management Information Base, Übersicht 96
MAPI, Unterstützung 85, 87
McAfee
  Firewall erzwingen 143
  Integration 91
Meeting Series
  Siehe Secure Meeting
Methode, Definition 92
MIB, Übersicht 96
Microsoft Authenticode-Zertifikat 72
Microsoft JVM*Siehe* JVM
Minor (Protokollmeldung), Definition 97
MS Exchange
  Abbildung 118
  Protokoll, Unterstützung 85
  Unterstützung 87
  Windows-Registrierung aktualisieren 118
Multicast-Synchronisierungsprotokoll 81

N

Namenssperrung, Unterstützung 216
NCP konfigurieren 141
Netegrity SiteMinder
  Siehe Authentifizierungsserver, SiteMinder
Netscape
  Cachesteuerungs-Header, Unterstützung 332
  JVM-Ausführung 72
  Mail, Unterstützung 88
  Messenger, Unterstützung 86
  Secure Meeting, Unterstützung 18
  Webserver 147
NetScreen Communication Protocol
  konfigurieren 141
NetScreen Support, Zusammenarbeit mit ??–418
NetScreen-Support ix
NetScreen-Support, Zusammenarbeit mit 413–??
Network Connect
  Abbildung 101
  Aktivierung und Konfiguration 369
  Konfiguration 24
  Ressourcenrichtlinien 42, 369
  Rollen 57
  Übersicht 23, 26, 99, 107
  Verwendung 100
Network Time Protocol verwenden 130
Netzmaske
  Benutzeranforderungen definieren 26
  Definition in Ressourcenrichtlinien 47, 50
  für externen Port 157, 161
  Konfiguration 158, 161
Netzwerk
  Einstellungen
    erstmalig 157
    Konfiguration 157
  Hostnamen für lokale Auflösung angeben 164
  Pakete, Sniffing 415
  statische Routen angeben 163
Neuschreiben
  Durchgangsproxy, Option 103, 339
  Remote-SSO (Option) 342
New PIN-Modus, Unterstützung 215
Next Token-Modus, Unterstützung 216
Nicht-IVE-Gäste
  Siehe Secure Meeting, Rollen
Nslookup-Befehl 417
NT-Domäne
  Siehe Authentifizierungsserver, Active Directory

NTML, Konfiguration 213
NTP verwenden 130
Nullserver
Siehe Authentifizierungsserver, anonymer Server

O

Operationsmodus, Access Series FIPS 10
Optimiertes NCP konfigurieren 141
Oracle, Unterstützung 104
Outlook Express, Unterstützung 86
Outlook, Unterstützung 86, 87, 88
J-SAM 116
OWA, Unterstützung 90

P

PassGo Defender RADIUS-Server, Konfiguration 243
Permanente Daten, Definition 79
Permissive Zusammenführung
Übersicht 58
Persönliche Firewall
mit Cachebereinigung verwenden 64
Unterstützung 91
Pfad
Definition in Ressourcenrichtlinien 47, 48, 49
Ping-Befehl 417, 458
Plattform hochstufen und herunterstufen 383
Pocket PC, Übersicht 7
POP
Clients 89
Mailserver 379
Unterstützung 85, 87, 90
Port
Anforderungen angeben 92
Definition in Ressourcenrichtlinien 51
extern, ändern 157, 161
Ports
Definition in Ressourcenrichtlinien 47
Post Office Protocol
Siehe POP
POST-Richtlinie, Übersicht 107
Pragma No-Cache (PNC, Header) 334
Privater Schlüssel
Import 147
Management 9
productName, MIB-Objekt 197
productVersion, MIB-Objekt 197
Protokoll, Definition in Ressourcenrichtlinien 46, 50
Protokollierung
Clientprotokolle
Cachebereinigung 65
Secure Meeting 21
Cluster 80, 81
Filter
Konfiguration 194
Übersicht 97
Formate
Konfiguration 194
Übersicht 97
Installationsprotokolle, Secure Meeting 21
Konfiguration 187
kritische Ereignisse 128
Protokolldateien speichern 188
Schweregrade 96
Übersicht 95
zu protokollierende Ereignisse angeben 189
Proxy
Siehe Durchgangsproxy

Q

Quell-IP-Einschränkungen konfigurieren 24, 25, 26

R

RADIUS
Siehe Authentifizierungsserver, RADIUS
Redundanz, Aktiv/Passiv-Modus 77
Regel
Bestandteil einer Ressourcenrichtlinie 43
Cachesteuerung 332
Definition 92
Konfiguration 52, 278
Regeln für die Zwischenspeicherung von Inhalten 332
Registrierung
Sicherheitsanforderungen, Definition 92
Registrierungseinstellungen
J-SAM 118

Remote-SSO
Konfiguration 342
Ressourcenrichtlinien 342
Remote-SSO (Option)
Übersicht 107
Remotesteuernder
Siehe Secure Meeting, Rollen
Ressourcen, Bestandteil einer Ressourcenrichtlinie 42
Ressourcenrichtlinien
Auswertung 43
Codierung 360
Datei 42, 351
Definition 5, 25
E-Mail-Client 42, 379
Export 395
Import 397
IP-Adresse 51
Java 336, 337
Konfiguration 325, 427
Network Connect 42, 369
Remote-SSO 342
SAM, SAM-Ressourcenrichtlinien 361
Secure Application Manager 42
Secure Meeting 42, 375
Selektives Neuschreiben 339
Server 50
Telnet/SSH 42, 365
Übersicht 41
UNIX/NFS-Dateien 49, 358
Verwaltung 269
vorkonfigurierte Richtlinien 5
Web 41, 46, 325
Windows-Dateien 48, 352
Zwischenspeicherung 331
Ressourcenrichtlinien für Zwischenspeicherung 331
Richtlinien
Anmelderichtlinien *Siehe* Anmelderichtlinien
Authentifizierungsrichtlinien *Siehe* Authentifizierungsrichtlinien
Ressourcenrichtlinien *Siehe* Ressourcenrichtlinien
Richtlinien für Java-Zwischenspeicherung 336
Rolle
Auswertung 58
Bestandteil einer Ressourcenrichtlinie 43
Definition 5, 24, 55
Export 395
Import 397
Konfiguration 427
Verwaltung 271
vordefinierte Rollen 5
Zugriffssteuerung für Webserver 330, 370, 373
Zuordnung 23, 35, 37, 58, 277
Zusammenführung 58
Rpc_Binding_Order (Registrierungseinstellung) 118
RSA ACE/Server
Hostnamenauflösung 36
Siehe Authentifizierungsserver, ACE/Server

S

SAM
Siehe Secure Application Manager
Schlüssel 147
privat, *Siehe* Privatschlüssel
Security World, *Siehe* Access Series FIPS, Security World-Schlüssel
sdconf.rec, Generierung 219
Secure Application Manager
Anwendungen für J-SAM konfigurieren 308
Anwendungen für W-SAM konfigurieren 305, 306
Hosts für W-SAM konfigurieren 305, 306
J-SAM
Abbildung 113
Definition 109
Übersicht 111
Verwendung 112
Konfiguration 24
Ressourcenrichtlinien 42
Rollen 57
Übersicht 109
W-SAM
Abbildung 111
Definition 109
Übersicht 109
Verwendung 110
zusätzliche J-SAM-Optionen 306
Secure Email Client
Siehe E-Mail-Client
Secure Meeting
Aktivierung 317
Aktivität anzeigen 126

Aktualisierungsoption 13
Appliance 13
Benachrichtigungs-E-Mails
Aktivierung 158
Beschreibung 15
Konfiguration 319
Fehlerbehebung 20
Konferenz-Betrachter 15
Konferenzen löschen 133
Konfiguration 24
Ressourcenrichtlinien 42, 375
Rollen 57
Ersteller 14
Gäste 14
Konferenzleiter 16
Remotesteuernder 16, 320
Teilnehmer 15
Sofortkonferenz 15
Textnachrichten 15
Übersicht 13
Überwachung 133
unterstützte Umgebungen 18
SecurID
Siehe Authentifizierungsserver, ACE
SecurID-Token
Siehe Authentifizierungsserver, ACE/Server, SecurID
Security World
Übersicht 9
Selektives Neuschreiben 339
Serielle Konsole
Access Series FIPS-Gerät initialisieren 9
Clustermitglieder hinzufügen 179
für Systemaufgaben verwenden 453
Server
Definition in Ressourcenrichtlinien 48, 49
für Authentifizierung verwendete Typen 36
Ressourcenrichtlinien 50
Siehe auch Authentifizierungsserver
Server Certificate (Registerkarte), Certificates (Menü) 147
Serverkatalog konfigurieren 279
Sicherheitsoptionen
Konfiguration 140
Sicherung von Netegrity Siteminder-Servern aktivieren 255
signedInWebUsers, MIB-Objekt 197
Simple Mail Transfer Protocol
Siehe SMTP-Mailserver
SiteMinder
Siehe Authentifizierungsserver, SiteMinder
Sitzungen beenden 132
Sitzungsparameter konfigurieren 56
Sitzungsrolle, Definition 58
Sitzungszeitbegrenzungen
Einfluss auf die Cachebereinigung 64
Konfiguration 24
Smart Caching 333
Smartcard
Siehe Access Series FIPS, Administratorkarte
SMSESSION-Cookies 247, 256
SMTP-Mailserver
Aktivierung 379
Unterstützung 85
Verwendung mit Secure Meeting 14
Snapshotdatei (zur Fehlerbehebung) 414
Snapshots erstellen 406
SNMP
Einstellungen angeben 196
IVE als Agent überwachen 195
Unterstützung 96
Sofortkonferenz
Siehe Secure Meeting, Sofortkonferenz
Software
herunterladen 129
Installation 385
Installation in einem Cluster 173
Speichernutzung, Anzeige 126
SSL
Beschleuniger 387
Handshakes
delegieren 387
Management 9
Navigation zu Sites 140
zulässige Verschlüsselungsstärke 140
zulässige Version 140
Standardformat für Protokolldatei 195
Statische Routen, Konfiguration 163
Statistikanzeige 200
Statussynchronisierung 79
Sun JVM
Siehe JVM
Sygate
Enforcement-API-Integration 91
Security Agent-Integration 91
Sicherheit erzwingen 143

Synchronisierungsprotokoll, Cluster 81
Syslog-Server konfigurieren 190
System
  Daten archivieren 403
  Fehlerbehebung 413, 414, 415, 417, 418
  Kapazität, Anzeige 126
  Konfiguration 383
  Konfiguration exportieren 389
  Konfiguration importieren 390
  Rollback 453–458
  Software installieren 385
  Statistikanzeige 200
  Statusdaten, Beschreibung 80

T

TCP-Dumpdatei (zur Fehlerbehebung) 415
Teilnehmer
  Siehe Secure Meeting, Rollen
Telnet/SSH
  Konfiguration 24
  Ressourcenrichtlinien 42, 365
  Rollen 57
Temporäre Dateien entfernen 63
Temporäre Daten, Definition 79
Textnachrichten
  Siehe Secure Meeting, Textnachrichten
THMTL, benutzerdefinierte Seiten erstellen 209
TLS
  zulässige Version 140
Traceroute-Befehl 417, 458
Traps
  Definition 96
  Konfiguration 196

U

Überprüfungs-URL 78
Übertragungsrate
  Konfiguration 158, 161
Uhrzeit und Datum einstellen 130
Unicast-Synchronisierungsprotokoll 81
UNIX
  Lesezeichen erstellen 301
UNIX/NFS-Datei
  Ressourcenrichtlinien 358
UNIX/NFS-Dateien
  Ressourcenrichtlinien
    Definition 49
Untergeordneter ACE/Server, Unterstützung 216
URL
  Zugriffsstatistik 200
URLs
  Anmelde-URLs festlegen 204
USER (Variable)
  in UNIX-Lesezeichen 301
  in Weblesezeichen 295
  in Windows-Lesezeichen 299

V

VeriSign-Serverzertifikat, Verwendung 71
Vermittlung
  Anmeldeinformationen, Benutzer 141
  Remote-SSO 342
  Selektives Neuschreiben 339
Verschlüsselung
  Beschreibung 4
  Stärke 140
Verzeichnisserver
  Siehe auch Authentifizierungsserver
  Definition 37
Virtuellen Hostnamen konfigurieren 17, 341
Virtueller Hostname, Konfiguration 158
Vorführender
  Siehe Secure Meeting, Rollen
Vorlagen, anpassbare Oberfläche 209
VPN ohne Client, Übersicht 99

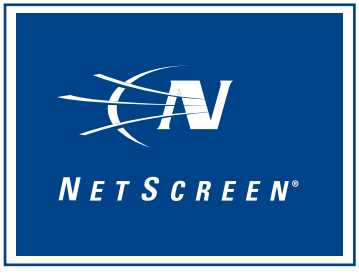
W

W3C-Format für Protokolldatei 195
Wartungsmodus, Access Series FIPS 10
Web
  Browsingprobleme 413
  Lesezeichen erstellen 295, 296, 299, 302, 312, 315, 316, 322
  Proxy angeben 348
  Ressourcenrichtlinien 41, 46, 325
  Rollenkonfiguration 56
  Serverzugriffssteuerung 330, 370, 373
  Spitzennutzungsstatistik 200

Zugriffssteuerung 330, 370, 373
Web-Agent, IVE als 252
Webbrowsing konfigurieren 24
Webkonsole
Beschreibung 8
Clustermitglieder hinzufügen 176
Startseite 67
Webproxy, Benutzer-PCs konfigurieren 311
WELF-Format für Protokolldatei 195
Windows
Anmeldeinformationen 355
Cachesteuerungs-Header, Unterstützung 332
Windows Internet Naming Service-Server, Konfiguration 159
Windows, Unterstützung
Secure Meeting 18
Windows-Datei
Ressourcenrichtlinien 352
Windows-Dateien
Ressourcenrichtlinien 48
Windows-Registrierung ändern 118
Windows-Unterstützung
J-SAM 113
Zertifikate 72
WINS
für externen Port 157, 161
Server, Konfiguration 159

Z

Zeitbegrenzungen
Siehe Sitzungszeitbegrenzungen
Zertifikat
Anforderung an Stammzertifikat 71, 153
Anmeldungen einschränken
Benutzer 432, 433
Appletzertifikat
Definition 69
Import 155
Übersicht 71
Attribute konfigurieren 278
Browsing einschränken 140
clientseitiges Zertifikat
Anforderung 70, 153
Definition 69
SiteMinder 249
Codesignaturzertifikat
Siehe Zertifikat, Appletzertifikat
Einschränkungen konfigurieren 24, 25
Empfehlungen zu Secure Meeting 20
JavaSoft 72
MS Authenticode 72
Richtlinien 432
Schlüssel
vorhandenes exportieren 147
vorhandenes importieren 147
selbst signiert 69
Server
Siehe Authentifizierungsserver, Zertifikatserver
Serverzertifikat
Definition 69
erneuertes Zertifikat importieren 150
vorhandenes exportieren 147
vorhandenes importieren 147
Zertifikatssignaturanforderung erstellen 151
Zertifikatssignaturanforderung importieren 152
Sicherheitsanforderungen festlegen 29
Signaturanforderung
Erstellung 151
Import 152
Zertifikat importieren 152
Sperrliste 5, 225
unterstützte Formate 69
verkettetes Zertifikat 71
Zwischenzertifikat 71
Zertifikatssignaturanforderung
Erstellung 151
Import 152
Zertifikat importieren 152
ZIP-Beschleuniger 387
Zone Labs
erzwingen 143
Integration 91
Zugriffssteuerung
Liste (ACL)
Export 395
Import 397
Webressourcen 330, 370, 373
Zugriffsverwaltung, Definition 23
Zulässige Rollen, Definition 38



©1998-2004 NetScreen Technologies, Inc.
All Rights Reserved